# Exhibit 3

PERSEREC

Technical Report 17-10
August 2017

# The Expanding Spectrum of Espionage by Americans, 1947 – 2015

Katherine L. Herbig, Ph.D.
*Northrop Grumman Technology Services*

OPA
OFFICE OF PEOPLE ANALYTICS

Approved for Public Distribution
Defense Personnel and Security Research Center
Office of People Analytics

NOTE: For correspondence about this report, please contact PERSEREC@mail.mil

**Technical Report 17-10** **August 2017**

# The Expanding Spectrum of Espionage by Americans, 1947 – 2015

Katherine L. Herbig, Ph.D.—*Northrop Grumman Technology Services*

Released by—Eric L. Lang, Ph.D.

Defense Personnel and Security Research Center
Office of People Analytics
400 Gigling Rd.
Seaside, CA 93955

NOTE: For correspondence about this report, please contact PERSEREC@mail.mil

# REPORT DOCUMENTATION PAGE

| **REPORT DOCUMENTATION PAGE** | **Form Approved OMB No. 0704-0188** |
|---|---|



| 1. REPORT DATE: | 2. REPORT TYPE Technical Report | 3. DATES COVERED: Sept. 2014 – Mar. 2017 |
|---|---|---|
| 4. The Expanding Spectrum of Espionage by Americans, 1947 – 2015 | 5a. CONTRACT NUMBER: | |
| | 5b. GRANT NUMBER: | |
| | 5c. PROGRAM ELEMENT NUMBER: | |
| 6. AUTHOR(S): Katherine L. Herbig, Ph.D. | 5d. PROJECT NUMBER: | |
| | 5e. TASK NUMBER: | |
| | 5f. WORK UNIT NUMBER: | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Defense Personnel and Security Research Center<br>Office of People Analytics<br>400 Gigling Road<br>Seaside, CA 93955 | 8. PERFORMING ORGANIZATION REPORT NUMBER<br>PERSEREC-TR-17-10 | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSORING/MONITOR'S ACRONYM(S) | |
| | 11. SPONSORING/MONITOR'S REPORT NUMBER(S): | |

12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited

13. SUPPLEMENTARY NOTES:

ABSTRACT: The report describes characteristics of 209 Americans who committed espionage-related offenses against the U.S. since 1947. Three cohorts are compared based on when the individual began espionage: 1947-1979, 1980-1989, and 1990-2015. Using data coded from open published sources, analyses are reported on personal attributes of persons across the three cohorts, the employment and levels of clearance, how they committed espionage, the consequences they suffered, and their motivations. The second part of the report explores each of the five types of espionage committed by the 209 persons under study. These include: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. The statutes governing each type are discussed and compared. Classification of national security information is discussed as one element in espionage. In Part 3, revisions to the espionage statutes are recommended in light of findings presented in the report.

14. SUBJECT TERMS:

| 15. SECURITY CLASSIFICATION OF: UNCLASSIFIED | | | 16. LIMITATION OF ABSTRACT: | 17. NUMBER OF PAGES: 227 | 19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director |
|---|---|---|---|---|---|
| a. REPORT: UNCLASSIFIED | b. ABSTRACT: UNCLASSIFIED | c. THIS PAGE: UNCLASSIFIED | | | 19b. TELEPHONE NUMBER (Include area code): 831-583-2846 |

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

# PREFACE

The Defense Personnel and Security Research Center (PERSEREC) dates from 1986. It was founded because of the espionage of John Walker and his ring of spies. Part of a record year for spies in 1985 in which 11 Americans were arrested for espionage, Walker's capture provoked outrage, as did the revelation that for 20 years he had betrayed the trust the U.S. Navy placed in him as a cryptographic radioman. A commission to investigate security practices then formed under General Richard G. Stilwell. Among its recommendations for improvement was the creation of an organization to perform behavioral science research on personnel security policies and practices, and so in 1986, the Department of Defense (DoD) established PERSEREC.

For 30 years, PERSEREC has worked to improve the effectiveness, efficiency, and fairness of DoD's personnel and industrial security systems. One consistent research focus has been the phenomenon of trust betrayal in crimes such as espionage. This report is the fourth in a series of unclassified reports based on information collected in the PERSEREC Espionage Database. Materials on espionage and espionage-related offenses, including attempted espionage, conspiracy to commit espionage, theft, and illegal collection of closely-held national defense information with the intent to commit espionage, have been coded into the database. A founding goal of PERSEREC is to improve security education and awareness, and so these reports are based on open sources in order to facilitate public access and broad distribution.

Eric L. Lang, Ph.D.
Director

# EXECUTIVE SUMMARY

This report is the fourth in the series on espionage by Americans that the Defense Personnel and Security Research Center (PERSEREC) began publishing in 1992. The current report updates earlier work by including recent cases, and it extends the scope by exploring related types of espionage in addition to the classic type. There are three parts to this report. Part 1 presents characteristics of Americans who committed espionage-related offenses since 1947 based on analyses of data collected from open sources. Part 2 explores the five types of espionage committed by the 209 individuals in this study: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. Each type is described by its legal bases, and examples of cases and comparisons with the other types of espionage are provided. Part 3 considers the impact of the changing context in which espionage takes place, and discusses two important developments: information and communications technologies (ICT) and globalization. Recommendations are offered for revisions to the espionage statutes in response to these accelerating changes in context.

Part 1 compares data across three cohorts of persons based on when the individual began espionage: 1947-1979 (the early Cold War), 1980-1989 (the later Cold War), and 1990-2015 (the post-Soviet period). As the Cold War recedes in time, the recent cohort offers the most applicable data for the present. Among the characteristics of the 67 Americans who committed espionage-related offenses since 1990:

- They have usually been male and middle-aged. Half were married.
- Reflecting changes in the population as a whole, they were more diverse in racial and ethnic composition, and more highly educated than earlier cohorts.
- Three-quarters have been civil servants, one-quarter military, and compared to the previous two cohorts, increasing proportions have been contractors, held jobs not related to espionage, and/or not held security clearances.
- Three-quarters succeeded in passing information, while one-quarter were intercepted before they could pass anything.
- Sixty percent were volunteers and 40% were recruited. Among recruits, 60% were recruited by a foreign intelligence service and 40% by family or friends. Contacting a foreign embassy was the most common way to begin as a volunteer.
- Compared to earlier cohorts in which the Soviet Union and Russia predominated as the recipient of American espionage, recent espionage offenders have transmitted information to a greater variety of recipients.
- Shorter prison sentences have been the norm in the recent past.
- Sixty-eight percent of people received no payment.

- Money is the most common motive for committing espionage-related offenses, but it is less dominant than in the past. In the recent cohort, money was a motive for 28%, down from 41% and 45% in the first and second cohorts, respectively. Divided loyalties is the second most common motive (22%). Disgruntlement and ingratiation are nearly tied for third place, and more people seek recognition as a motive for espionage.

Returning to the full population, the majority of the 209 individuals committed classic espionage in which controlled national security information, usually classified, was transmitted to a foreign government. Classic espionage predominates in each cohort, but declined from 94% the first cohort to 78% in the most recent. This reflects authorities' recent increasing treatment as espionage of the four additional types discussed in Part 2: leaks; acting as an agent of a foreign government; violations of export control laws; and economic espionage. Each of the four additional types is prosecuted under its own subset of statutes, which differs from those used in cases of classic espionage. The various types are usually handled by different federal agencies. They also differ in how involved the information of private companies and corporations is alongside government agencies.

The five types of espionage are not mutually exclusive, and a person may be charged with and convicted of more than one type. The assumption that espionage consists simply of classic espionage should be reexamined in light of how these four additional crimes are similar to or even charged as identical to classic espionage. All five types impose losses of national defense information, intellectual property, and/or advanced technologies that cause grave damage to the security and economy of the nation.

Four elements frame the analyses in Part 2. First, the legal statutes that define the crimes are identified and described. Prosecutorial choices as to which statutes to use are considered, alternate statutes that have been used in similar circumstances are identified, and reasons for the choices suggested. Second, examples of each type of espionage are presented as case studies. Third, issues resulting from classification of information are identified and discussed for each type, if applicable. Fourth, the numbers of individuals among the 209 are presented in tables for each of the five types, along with descriptive statistics to identify trends over time.

Part 3 discusses these trends by recognizing two central dimensions of the current context in which espionage occurs: ICT and globalization. Spies have moved with the times, and they employ all the technological sophistication and advantages they can access. Implications from this changing context are discussed, including how American espionage offenders gather, store, and transmit intelligence to a foreign government, and how a foreign government may now steal controlled information directly across interconnected networks, threatening to make spies obsolete.

Globalization affects many dimensions of life, and is especially apparent in areas relevant to espionage, such as political and military affairs, development of defense technologies, and international finance. It can influence the recruitment of spies and the likelihood that people will volunteer to commit espionage as a consequence of the ongoing trend toward a global culture, with its easy international transmission of ideas, civic ideals, and loosening allegiances of citizenship.

This report concludes by recommending revisions to the espionage statutes (Title 18 U.S.C. § 792 through 798) in order to address inconsistencies and ambiguities. Based on provisions enacted in 1917 and updated in last 1950, they are outdated. Three approaches to revision are outlined. First, try to eliminate inconsistencies among the espionage statutes themselves. Second, consider how to update the espionage statutes to reflect the current context of cyber capabilities, the Internet, and globalization. Third, consider how to amend the statutes that apply to all five types of espionage discussed in this report to reconcile inequities, eliminate gaps or overlaps, and create more consistency in the legal response to activities that are similar, even though they take place in different spheres.

In an appendix, this report examines how espionage fits into the broader study of insider threat, and considers three insights from insider threat studies that may illuminate espionage: personal crises and triggers, indicators of insider threat, and the role of organizational culture.

# TABLE OF CONTENTS

TABLE OF CONTENTS



## LIST OF TABLES

## LIST OF FIGURES



## LIST OF TABLES IN APPENDICES



## LIST OF FIGURES IN APPENDICES

# INTRODUCTION

This is the fourth technical report in the series on espionage published by the Defense Personnel and Security Research Center (PERSEREC). The reports have been based on a For Official Use Only (FOUO) database developed by PERSEREC over 30 years.[1] In its approach, this report shares with the three earlier reports many of the database variables discussed, yet it also differs in that it reflects the concerns of this time, and thus, it takes up the issues and challenges of the early 21st century.

## BACKGROUND

The first PERSEREC espionage report, published in 1992, looked at 117 American citizens who had committed espionage during the Cold War. In it, findings were compared by trait. For example, the authors looked at civilian versus military spies, volunteers versus recruited spies, and successful versus unsuccessful spies. They then applied these results to issues such as improving the personnel security system, the changing motivations for espionage, and explaining the sudden increase of espionage by Americans in the 1980s (Wood & Wiskoff, 1992).

The second report in the series was published a decade later in 2002. By then the number of Americans convicted of espionage or espionage-related[2] offenses had grown to 150. The report followed the analytical scheme of the first by comparing traits, but it discussed in some depth new issues shaping the context of espionage, including: the history of Soviet espionage in the U.S. and the impact of the Soviet Union's collapse; shifting policies on the prosecution of espionage; technological advances that were reshaping information storage and communications; and globalization's effects on national allegiances (Herbig & Wiskoff, 2002).

The third PERSEREC espionage report was published in 2008, when there were 173 Americans to consider. This report shifted the analytical focus from the traits of the earlier reports to emphasize changes over time. Instead of looking at the population by military versus civilian or volunteer versus recruited spy, people were divided into three cohorts based on when they began espionage and analyzed accordingly. For example, the number of volunteers versus the number of recruits was compared across the three cohorts: those who began between 1947 and 1979 (the early Cold War), those who began between 1980 and 1989 (the later Cold War), and those who began between 1990 and 2015 (the post-Soviet period). Because so many Americans began attempting espionage during the 1980s—and demographically they were a distinctive cohort—this decade was called out separately.

---

[1] The PERSEREC Espionage Database contains information that is designated For Official Use Only (FOUO) as well as personally identifiable information, and therefore, the database itself is FOUO.

[2] Espionage-related offenses are those not charged under the espionage statutes but under related statutes that nonetheless punish crimes identical in important respects to espionage.

Comparisons across cohorts produced findings about how traits among spies had changed over time. Since the terrorist attacks of 9/11 shaped so many aspects of life in the U.S., including espionage, this report highlighted the 11 persons who had spied since 9/11 in short case studies. New issues discussed in the third report reflected 9/11's impact: the context of global terrorism; homegrown terrorists; the impact of terrorism on espionage; the application of the expanding capabilities of the Internet for espionage; and the strain placed on American espionage statutes by trying to prosecute non-state groups or their supporters using laws from 1917 (Herbig, 2008).

As of 2015, 209 American citizens were convicted of espionage or espionage-related crimes. While 36 individuals have been entered into the PERSEREC Espionage Database since the third report was published in 2008, not all 36 began espionage or even were arrested between 2008 and 2015. Some earlier spies only came to light since 2008, such as Marta Velazquez, and a few earlier spies have been added as materials became available. This fourth report follows the analytical conventions of the third in that it divides 209 people into three cohorts based on when they began espionage: between 1947 and 1979, between 1980 and 1989, and between 1990 and 2015. The goals of this report are to understand espionage by Americans, to discern changes over time, to explore the five types of espionage these individuals represent, and to suggest trends that may guide successful countermeasures.

Some issues raised in earlier reports have expanded or deepened since 2008; others are new. Domestic terrorist attacks and sabotage have come to be framed as insider threats, reflecting the attacks on fellow U.S. citizens at Fort Hood, Texas, and the Washington Navy Yard, and espionage is often folded into this more encompassing description. Enemies in cyberspace have become more sophisticated. Economic espionage, merely mentioned as a threat in 2008, has grown and now challenges classic espionage (i.e., seeking national defense information) as a serious threat to national security. The People's Republic of China (PRC) continues to perfect its unique approach to espionage and continues to profit from it. And, the phenomenon of leaks (i.e., providing secrets to the press or the public who then provides them to everyone) exploded onto the scene with the actions of Bradley (Chelsea) Manning, Edward Snowden, and the unprecedented number of resulting prosecutions since 2009. These issues help form the current context for espionage that will be considered here.

The PERSEREC Espionage Project has three elements. The PERSEREC Espionage Database currently holds electronic data on 209 individuals whose activities span the 68 years from 1947 to 2015. Second, each individual in the database has a corresponding hard copy file with information from press accounts, scholarly articles, and books. Third, PERSEREC publishes unclassified reports, which allows for wider distribution to any government agency and to those in the public interested in following specific cases or learning more about espionage in general.

The 209 individuals in the PERSEREC Espionage Database were convicted or initially prosecuted for espionage, conspiracy to commit espionage, attempting to commit espionage, or for whom evidence of espionage or intent to commit espionage exists, even though for various reasons the person was not or, in a few cases, has not yet been convicted of those crimes. This latter category includes people who defected or died, who were given immunity from prosecution, or who plea bargained to lesser charges. Prosecutors often agree to plea bargains in espionage cases in exchange for information, either because evidence required by some espionage statutes is lacking or to protect counterintelligence methods or classified information from being discussed in open court. Lesser charges in plea bargains typically include conspiracy to communicate national defense information to a foreign government, acting as an agent of a foreign government, theft of government property, conspiracy to gather information knowing it would be useful to a foreign government, or even simple mishandling or improper storage of classified documents.

Outcomes of espionage cases are influenced not only by the charges against the offender and the plea bargaining undertaken on his or her behalf, but also by prosecutorial choices and policies. The 2002 PERSEREC espionage report discussed trends in prosecution policies in some depth (Herbig & Wiskoff, 2002). A noticeable trend in the prosecution of recent cases has been the increasing number of offenders not charged with espionage, but with acting as unregistered agents of a foreign power. The espionage statutes demand more stringent evidence of mental states and intentions for conviction than does acting as an agent of a foreign power, which may explain why, since 2001, twice as many individuals have been charged with acting as an agent of a foreign power as in any earlier decade.

Current criteria for inclusion as a case in the PERSEREC Espionage Database are:

(1) Individuals convicted of espionage or conspiracy to commit espionage, or for attempting espionage, or for admitting that they intended to commit espionage;

(2) Individuals prosecuted for espionage but who committed suicide before the trial or sentencing could be completed;

(3) Individuals for whom clear evidence of espionage (actual or attempted) existed, even though they were not prosecuted. This category includes cases involving defections, deaths at early stages in an investigation, and those administratively processed (e.g., allowed to retire, given immunity, exchanged, or discharged from the military);

(4) Individuals for whom clear evidence of actual or attempted espionage existed and who were initially charged with espionage-related crimes, but who were prosecuted for an offense other than espionage, such as mishandling classified information, as a result of plea bargaining; and

(5) Individuals charged with acting as unregistered agents of a foreign power, and for whom evidence exists that they collected and then intended, attempted, or succeeded in passing information to that foreign power.

## ORGANIZATION OF THE REPORT

This report is divided into three parts. Part 1, Characteristics of Espionage by Americans, reports findings based on analyses of 209 individuals who committed espionage-related crimes. Part 2, Types of Espionage, explores in detail the five types of espionage these 209 individuals committed, and provides examples and analyses from collected data. Part 3, Context and Recommendations, considers changes in the context of espionage, how these changes shape espionage, and how they require revisions to the statutes that govern it.

Part 1 first compares people across time periods (1947-1979, 1980-1989, and 1990-2015) based on when they began espionage-related activities, and then explores selected traits and how they apply to contemporary issues. An assumption underlies the decision to focus on when a person began espionage, which is that in important ways, an individual's choice of action is influenced by the context of the time and place in which the person lives. On the one hand, the ways in which it was possible to commit espionage in 1955 differed quite dramatically from the ways espionage could be committed in 1985, and it was different again in 2015. On the other hand, basic elements of the crime of espionage persist across any period. The basic and necessary elements for committing espionage include opportunity, conception, motive, lack of internal constraints, and ineffective external constraints (Herbig, 1994). It is because such basic elements can be found in any act of espionage that one instance can be compared with other instances to derive analytic categories and patterns that will be instructive across cases from any period. Yet, it is equally important to capture the very real changes over time.

Two events mark the time periods in which espionage has been analyzed in this study. One event is the collapse of the Soviet Union, from the fall of the Berlin Wall in November 1989 to the dissolution of the Soviet Union as a government in December 1991. In this report, 1990 serves as the turning point within that time. The second event that marks an abrupt shift in context is 9/11. Since then, implications from those attacks have been and still are unfolding.

Before the Soviet Union fell apart, it competed with the U.S. for more than four decades and it was the foremost customer for espionage by Americans. Having one main adversary and customer for American intelligence, and having it be the Soviet Union, shaped the context for espionage in the first two time periods studied here.

After the 9/11 attacks focused the nation's attention on the growing threat from global terrorism, it became apparent that Islamic terrorists who were organized in internationally-networked cells posed a new, transnational intelligence threat. It is a threat whose challenges can be quite different from the Cold War parameters of two competing superpowers. Changes since 9/11 in the context of espionage—in the collection of intelligence, the creation of new agencies to respond, and the new challenges from cyberspace—have reshaped the espionage game.

This report attempts to identify and highlight the counterintelligence implications of the cases of espionage discussed. If available, information was collected on: personal traits that could serve as triggers for espionage; personnel security concerns as defined by the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information; indicators that espionage was in progress, such as unexplained affluence; and details about motivations, methods of transmission, and how people were caught (Berger, 1997). Open sources are often deliberately vague about counterintelligence details and on the fine points of more obscure spies' lives, but all available open source information was sought and collected to offer a starting point for counterintelligence analysis.

In Part 1, results are usually first reported in tables. The text accompanying the tables highlights certain results. Discussion is integrated into each section and includes implications, case examples, and other observations. Most of the examples come from the third cohort, individuals who began their activities since 1990, and especially those who began since the last report was published in 2008. Persons in this most recent group are new to this series and have not been discussed in prior reports. Some of the examples have been developed into brief thumbnail sketches to illustrate a trait or to provide materials for increased public awareness.

Part 2 examines the five types of espionage that comprise the expanding spectrum of espionage by Americans: classic espionage, leaks, acting as an agent of a foreign government, violations of export control laws, and economic espionage. Each type is discussed in terms of the applicable statutes, explored in terms of how it is similar to and different from the classic type, and illustrated by example cases. Each type is summarized using a common figure drawn from classic espionage to highlight commonalities among the types of espionage.

Part 3 describes the current context of espionage by Americans by focusing on two developments: information and communications technology (ICT) and globalization. These shape the environment in which spying now takes place. This section concludes by considering how, in light of the earlier sections, the espionage statutes need to be revised. Three approaches to revision are suggested.

A discussion of how the study of espionage may be enriched by studying selected works on insider threat appears in Appendix A. For a list of the names and selected characteristics of the 209 individuals included in this study, see Appendix B.

## METHOD

Information was compiled from newspaper and magazine accounts, biographies, general published works on espionage, and collections of case histories compiled by other researchers. Online research tools were consulted, such as Google Scholar and CICentre.com. Missing information was sought in the classified investigative files of several federal agencies that could confirm what was known, but only unclassified information has been maintained in the PERSEREC Espionage Database.

As in the earlier versions of the database, five categories of information were gathered on individuals identified for inclusion: biographical, employment and security clearance, characteristics of espionage, motivation, and consequences. Within these categories, variables were selected that would be available largely from open sources and would provide a rich array of background data on spies. Included were personal and demographic information, aspects of the job environment, access to classified information, how people first got involved with espionage, how their careers as spies evolved, how they operated as spies, and how their spying careers ended. Some variables were included for identification and documentary purposes only and were not used for analysis. Some were qualifying descriptors for other variables (e.g., *foreign relative qualifier* provides details about the previous variable, *foreign relative*, which is coded Yes, No, or Unknown).[3]

Data were coded into variables by several coders over time. A detailed codebook was used to guide decisions and judgments during the coding.

The 209 individuals discussed here constitute a very small number on which to apply statistical analysis. Descriptive statistics, with a comparison of frequencies, are the simple analytical tools used here on such small numbers that do not support more sophisticated techniques. While undoubtedly there are more instances of espionage by Americans that have not been made public, and still more that have not been uncovered, these 209 represent the known instances described in open sources that meet the criteria for inclusion defined here.

[3] More details on the coding procedures and considerations can be found by consulting the second report (Herbig & Wiskoff, 2002).

# PART 1

# CHARACTERISTICS OF ESPIONAGE BY AMERICANS

## PERSONAL ATTRIBUTES

The first dimension to consider in how espionage by Americans may have changed over time since 1947 is the personal attributes of the individuals: gender, race, age when they began espionage, level of education, marital status, and sexual orientation. Table 1 reports findings on these characteristics.

**Table 1**
**Personal Attributes**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=68* | *%* | *n=74* | *%* | *n=67* | *%* |
| Gender | | | | | | |
| Male | 65 | 95 | 65 | 88 | 61 | 91 |
| Female | 3 | 5 | 9 | 12 | 6 | 9 |
| Race/Ethnicity[4] | | | | | | |
| White | 58 | 85 | 60 | 81 | 37 | 55 |
| Black | 5 | 7 | 2 | 3 | 4 | 6 |
| Arab | 2 | 3 | 2 | 3 | 6 | 9 |
| Asian | 2 | 3 | 4 | 5 | 10 | 15 |
| Hispanic | 1 | 2 | 5 | 7 | 10 | 15 |
| Native American | 0 | 0 | 1 | 1 | 0 | 0 |
| Age when espionage began | | | | | | |
| Less than 20 | 3 | 4 | 7 | 10 | 0 | 0 |
| 20 to 29 | 23 | 34 | 34 | 46 | 11 | 16 |
| 30 to 39 | 26 | 38 | 15 | 20 | 22 | 33 |
| 40 or more | 16 | 24 | 18 | 24 | 34 | 51 |
| Education, in years[5] | *(n=66)* | | *(n=68)* | | *(n=40)* | |
| 10 years | 4 | 6 | 5 | 7 | 0 | 0 |
| 12 years | 23 | 35 | 25 | 37 | 12 | 30 |
| 14 years | 13 | 20 | 13 | 19 | 4 | 10 |
| 16 years | 17 | 26 | 10 | 15 | 10 | 25 |
| 18 or more years | 9 | 13 | 15 | 22 | 14 | 35 |

[4] These are categories based on descriptions from open sources. They do not reflect a person's self-identification and they do not use U.S. Census categories. White, African-American or Black, Asian, and Native American are commonly used racial categories. Arab and Hispanic may be ethnic, cultural, or linguistic categories for people of various races. (For a discussion of these issues, see Cohn & Caumont, 2016.)

[5] There are more missing data for education than for many variables, especially in the third cohort, which makes conclusions about that cohort more tentative. Of the 27 persons in the third cohort whose level of education is unknown, 13 are naturalized citizens who may have been educated abroad, and the difficulty in tracking that information may account for some of the missing education data.

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| Marital status when espionage began[6] | | | *(n=69)* | | *(n=58)* | |
| Married | 48 | 70 | 35 | 51 | 33 | 57 |
| Single | 16 | 24 | 26 | 38 | 16 | 28 |
| Separated or divorced | 4 | 6 | 8 | 11 | 9 | 15 |
| Sexual orientation | *(n=61)* | | *(n=55)* | | *(n=57)* | |
| Heterosexual | 57 | 93 | 53 | 96 | 56 | 98 |
| Homosexual | 4 | 7 | 2 | 4 | 1 | 2 |

American spies continue to be overwhelmingly male—91% in the most recent cohort. Other personal attributes, however, have changed with time. As the population of the U.S. has become more diverse, so, too, has the population of spies. Whites are no longer so predominant at 55% of the total in the most recent cohort, compared with 85% in the earliest cohort. Since 1990, American citizens of Arab background have increased to 9%, and more Asians and Hispanics have attempted espionage. Asian Americans were 13% of the recent cohort and Hispanic Americans were 15%.

The 60% of recent spies for whom the level of education is known mirrors a trend in the general population. Recent spies appear to be better educated than the previous two cohorts, with 35% educated beyond high school and another 35% with postgraduate degrees. By comparison, according to the 2010 Census, 89% of native-born citizens 25 years or older in the U.S. held a high school degree or higher, including 28% with bachelor's degrees. Among the foreign-born naturalized citizens in 2010, 68% were high school graduates or higher, including 27% with bachelor's degrees (Grieco, et al, 2012). The most recent cohort appears to be the best-educated yet.

The general trend in American society over the past 60 years has been toward more divorce. Divorce rates doubled among people over 35 between 1990 and 2008, although they leveled off during the same period among younger people (Kennedy & Ruggles, 2014). Spies reflect that trend, with a rising rate of divorce that was interrupted during the 1980s when there were more young and single military spies. In the earlier two cohorts, 6% and 11% were divorced, while 15% of the recent group of spies was divorced.

Espionage remains a man's crime. Only 18 of the 209 American spies are women. Within cohorts, there were more women spies during the 1980s than in the earliest or most recent cohorts. Like many crimes, espionage entails taking risks, and if we extrapolate from crime and other risky behaviors in general, we can expect that espionage would likewise have a skewed gender ratio. More men than women

[6] There are more missing data for marital status than for some variables, especially for the third cohort; marital status for 9 of the 67 persons in the third cohort is unknown. This makes conclusions about that cohort's marital status more tentative.

commit crimes of all kinds. More men than women engage in risk-taking, such as interpersonal violence, dangerous sexual behaviors, risky sports, gambling, or risky maneuvers on the highways that result in accidents (Harris, Jenkins, & Glaser, 2006; Heuer, Jr., 1992).

Men also have more opportunity for espionage. Four times as many men are in government and military jobs that grant access to national defense information and to highly classified secrets (ClearanceJobs, 2012). More men than women are experts in computer hacking or cyber security (Landivar, 2013), and more men than women are highly placed in corporations (Warner, 2014).

Marta Rita Velazquez, a successful spy for decades for Cuba, was an exception to the preponderance of male spies. Her espionage only became publicly known in 2013, but by then she had been an agent and source for Cuba for 30 years. The Cuban Intelligence Service (CIS) recruited Velazquez in 1983 to be an agent early in her graduate studies at the Johns Hopkins University School of Advanced International Studies. In 1984, she met Ana Belen Montes, who was studying there part-time for an international career. They became friends, and Velazquez spotted, assessed, and recruited Montes for the CIS (United States District Court for the District of Columbia, 2004).

In March 1985, Velazquez and Montes traveled to Cuba for intelligence training. First they flew to Madrid, where they met Cuban agents and picked up false passports to use for a flight to Prague. More agents met them in Prague and provided two more false passports and clothing in which they flew to Cuba. It was illegal then for Americans to travel to Cuba under the embargo, requiring this subterfuge. The CIS training in Cuba covered communications using encrypted high-frequency radio broadcast messages, operational security measures, and practice polygraphs to inoculate the two agents against revealing themselves. To return, they retraced their steps via Prague and Madrid using their false passports, and once back in the U.S., they took up careers as successful civil servants and Cuban spies.

Starting in 1989, Velazquez worked as an attorney advisor for a series of government agencies, including the Department of Transportation, the U.S. Agency for International Development, and the Department of State (DoS). During the 1990s, Velazquez sent Top Secret (TS) information and the identities of at least two American intelligence agents to the CIS using her radio, and continued to spot potential agents (United States District Court for the District of Columbia, 2004).

Her real success as a spy, however, was in recruiting Montes, since Montes went on to become the top intelligence official on Cuba for the Defense Intelligence Agency. Her reports to Cuba over 17 years seriously damaged American intelligence. Montes was arrested on September 21, 2001 in a reaction rushed by the 9/11 attacks and concern that Montes would pass on plans for the American response. In March 2002, she pled guilty to espionage and began to cooperate with authorities. Three

months later, Velazquez resigned her government position in the U.S. embassy in Guatemala and abruptly moved to Sweden, where she continues to live secure from extradition. The Federal Bureau of Investigation (FBI) learned of Velazquez from Montes during her 2002 debriefings and indicted her in 2004. The FBI only notified Velazquez in 2010 that she is under suspicion of espionage, and only publicly unsealed her indictment in April 2013 (United States District Court for the District of Columbia, 2004; Venteicher, 2013; Popkin, 2013).

Recently, American spies have been older when they began their espionage activities. In the first cohort that began spying between 1947 and 1979, 38% were under 29 years old, while in the second cohort, 56% were under 29. The recent cohort that started between 1990 and 2015 shows decided aging: no one was under 20, only 16% were between 20 and 29, and over half were 40 or older.

Benjamin Pierce Bishop is an example of the greying American spy. He was 59 in June 2011 when he met a 27-year-old Chinese graduate student at an international defense conference in Hawaii. They became friends, then lovers. She asked him for advice and sources for her research, and he began to bring classified documents home to review before answering her questions. Eventually, he emailed answers to her that included classified national defense information, and he talked about other issues with her, including details of a meeting classified as Secret between the U.S. and South Korea, nuclear war plans and strategies, early warning radar systems, missile defense systems, and strategic resources and resource locations (United States Attorney's Office District of Hawaii, 2014).

Bishop had recently retired as a Lieutenant Colonel in the U.S. Army and was working as a contractor at the U.S. Pacific Command at Camp H.M. Smith on the island of Hawaii. He held a Top Secret with SCI access (TS-SCI) security clearance and served as a planner and specialist in cyber defense. His wife and daughter had remained in Utah while he worked on assignment in Hawaii, but in 2012, he asked for a divorce, explaining that he had met someone else. The requirements of his clearance specified that he disclose all of his contacts with foreign nationals and any travel he undertook that included such contacts. Bishop, however, changed the name of his lover on his disclosure forms to a masculine variation to hide their affair and her identity (Zimmerman, 2014).

He was arrested on March 15, 2013, and charged with two counts of espionage, willfully disclosing classified national defense information to someone not authorized to receive it, and illegally retaining classified national defense information at home. He pled guilty and was sentenced on September 17, 2014, to 87 months (7 years and 3 months) in prison plus 3 years of supervised release (Former U.S. Officer, 2014). The press pronounced that Bishop had fallen into a honey trap, a snare set by a young woman to lure an older man into a romance for profit and access to classified information. The Chinese national was not charged and her name was not revealed by the prosecution. At his sentencing, Bishop's lawyer blamed his reckless actions on love, saying, "There was no intent to harm

the U.S. He made an error, a serious error in judgment for the love of a woman" (Semko, 2013; Zimmerman, 2014).

In general, recent persons convicted of espionage-related offenses have been male, middle-aged, well-educated, and of a variety of racial and ethnic backgrounds that mirrors the increasing level of education and diversity of American society.

## EMPLOYMENT AND CLEARANCE

The jobs individuals perform and the level of security clearance they hold largely determine whether they will have the opportunity to commit espionage. Table 2 reports trends across the three cohorts in the proportions of civil servants, contractors, and uniformed military, along with military ranks, types and fields of employment, and levels of security clearance.

**Table 2**
**Employment and Clearance**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=68* | *%* | *n=74* | *%* | *n=67* | *%* |
| Civilian or uniformed military | | | | | | |
| Civilian (civil servants and contractors) | 34 | 50 | 39 | 53 | 51 | 76 |
| Uniformed military | 34 | 50 | 35 | 47 | 16 | 24 |
| Rank of uniformed military | | | | | | |
| E1 – E3 | 3 | 9 | 10 | 28 | 3 | 19 |
| E4 – E6 | 16 | 47 | 18 | 51 | 4 | 25 |
| E7 - WO | 10 | 29 | 3 | 9 | 3 | 19 |
| Officer | 4 | 12 | 2 | 6 | 4 | 25 |
| Unknown | 1 | 3 | 2 | 6 | 2 | 12 |
| Type of employment during espionage | | | | | | |
| Uniformed military | 34 | 50 | 35 | 47 | 16 | 24 |
| Civil servant | 15 | 22 | 16 | 22 | 15 | 22 |
| Government contractor | 8 | 12 | 8 | 11 | 14 | 21 |
| Job unrelated to espionage | 11 | 16 | 15 | 20 | 20 | 30 |
| Unknown | 0 | 0 | 0 | 0 | 2 | 3 |
| Occupational field when espionage began | | | | | | |
| Communications/intelligence | 25 | 37 | 23 | 31 | 12 | 18 |
| General/technical | 10 | 15 | 22 | 30 | 11 | 16 |
| Scientific/professional | 18 | 26 | 12 | 16 | 18 | 27 |
| Functional support/administrative | 12 | 18 | 10 | 14 | 9 | 14 |
| Miscellaneous | 3 | 4 | 7 | 9 | 17 | 25 |
| Security clearance when espionage began | | | | | | |
| TS-SCI | 10 | 15 | 11 | 15 | 14 | 21 |
| TS | 28 | 41 | 20 | 27 | 12 | 18 |
| Secret | 12 | 18 | 16 | 22 | 11 | 17 |
| Confidential | 1 | 1 | 3 | 4 | 0 | 0 |
| None held during espionage | 12 | 18 | 21 | 28 | 29 | 43 |
| Unknown | 5 | 7 | 3 | 4 | 1 | 1 |

## EMPLOYMENT AND CLEARANCE

Table 2 shows that occupations we would expect to present opportunities to commit espionage, such as communications and intelligence, actually declined by half after 1990, from 37% and 31% in the two earlier cohorts to 18% in the most recent. The number of spies in functional support or administrative occupations stayed about the same across time, while the influx of young military spies in the 1980s caused the proportion of general or technical occupations to spike for the second cohort. The proportion of scientific or professional occupations decreased in the 1980s, and then returned to 27% of the total, a level similar to the first cohort.

In the recent past, espionage has become a civilian's crime. The proportion of civilians increased from half in the first cohort to 76% in the most recent cohort. Among the uniformed military, there was a shift in the recent past toward equal opportunity across ranks. From a predominance of the lower enlisted ranks in the first two cohorts, the recent cohort has a higher proportion of senior enlisted and more officers at 25%.

The greater proportion of civilians coincides with two other trends in the type of occupations held during espionage. One is an increase in the number of spies who were government contractors: from 12% and 11% in the first two cohorts to 21% in the third cohort. This increase likely reflects the expanded hiring of contractors after 9/11 and the consequent increase in the proportion of clearances held by contractors in intelligence and defense roles (Sanger & Peters, 2013; Security from Within, 2013).

The second related trend is an increase in the number of spies in jobs apparently unrelated to espionage; frequencies doubled between the first cohort and the third. This is reflected in a notable increase in spies with miscellaneous occupations that would seem to have little to do with espionage and, on the surface, would not provide an opportunity to commit such a crime. From 4% and 9% in the two earlier cohorts, miscellaneous types of employment increased among recent spies to one-fourth of the total. Table 3 lists the miscellaneous occupations in the three cohorts.

**Table 3**
**Miscellaneous Occupations of Espionage Offenders**

| 1947-1979 | 1980-1989 | 1990-2015 |
|---|---|---|
| 1. unemployed | 1. unemployed | 1. boat pilot |
| 2. drug dealer | 2. public relations | 2. housewife and student |
| 3. retired | 3. shoe salesman | 3. Taekwondo instructor |
| | | 4. retired |
| | | 5. housewife and mother |
| | | 6. go-between, entrepreneur and organizer |
| | | 7. truck driver |
| | | 8. shop owner |
| | | 9. Chinese furniture importer |
| | | 10. pizza parlor clerk |
| | | 11. laborer and escort |
| | | 12. trader and importer of Middle Eastern foodstuffs |
| | | 13. airline gate agent |
| | | 14. unemployed broker of military equipment |
| | | 15. car dealer |
| | | 16. supervisor at aluminum door and window frame company |
| | | 17. menial jobs allowing observation of military installations |

Changes in the level of security clearance held by espionage-related offenders show a trend toward unclassified but sensitive information. (These data are reported in Table 2.) Persons with a clearance level of TS-SCI comprised 15% in the first two cohorts, and this increased slightly to 21% in the recent cohort. The proportion of those holding TS level clearances declined with each cohort: from 41% to 27% to 18% in the most recent cohort. Secret level clearances remained similar across time at 18%, 22%, and 17%. There were few Confidential clearances among espionage offenders, and this disused clearance level disappears from the recent cohort. The proportion of persons who held no security clearance while committing an espionage-related offense increased over time, from 18% to 28% to 43% in the recent cohort.

### Espionage Offenders without Security Clearances

The expectation of spies is that they have betrayed classified information. This is not consistently the case. Table 4 lists, by name, the 62 espionage-related offenders who did not hold security clearances or have access to classified information when they began committing an espionage-related offense. It also reports the methods they used to access information or the type of information they offered, and the outcome or sentence the person received.

**Table 4**
**Espionage Offenders with No Security Clearance When Espionage Began**

| Decade Began Espionage | Name | Method of Access or Type of Information in the Case | Outcome or Sentence |
|---|---|---|---|
| 1940s | Rees, Norman | Passed unclassified information[7] | Suicide |
| 1950s | Borger, Harold | Had accomplice with classified access | 2.5 years in prison |
| | Cascio, Guiseppe | Had accomplice with classified access | 20 years in prison |
| 1960s | Harris, Ulysses | Had accomplice with classified access | 7 years in prison |
| | Sattler, James | Passed unclassified information | Defection |
| 1970s | Lee, Andrew | Had accomplice with classified access | Life in prison |
| | Harper, James | Had accomplice with classified access | Life in prison |
| | Clark, James | Had accomplice with classified access | 12 years 8 months in prison |
| | Stand, Kurt | Had accomplice with classified access | 17 years and 6 months in prison |
| | Tumanova, Svetlana | Passed unclassified information | 1.5 years in prison |
| | Alvarez, Carlos | Passed unclassified information | 5 years in prison and 3 years of probation |
| | Barnett, David | Relied on his memory of classified information | 18 years in prison |
| 1980s | Pickering, Jeffrey | Stole classified information | 5 years in prison |
| | Jeffries, Randy | Stole classified information | 3 years in prison |
| | Kota, Subrahmanyam | Stole classified information | 1 year in prison and 3 years of probation |
| | Wilmoth, James | Had accomplice with classified access | 35 years in prison, reduced to 15 years |
| | Wolff, Jay | Stole classified information | 5 years in prison |
| | Davies, Allen | Relied on his memory of classified information | 5 years in prison |
| | Slavens, Brian | Relied on his memory of classified information | 2 years in prison |

[7] It is not necessary to transmit classified information to be convicted of espionage under espionage statutes. The main espionage statutes (Title 18 U.S.C. § 792-798) were passed in 1917 and do not mention classification, which was not applied until 1940, and there are numerous other statutes often applied to espionage-related crimes that also do not require information to be classified. These issues are discussed in detail later.

| Decade Began Espionage | Name | Method of Access or Type of Information in the Case | Outcome or Sentence |
|---|---|---|---|
| | Howard, Edward | Relied on his memory of classified information | Defection |
| | Smith, Richard | Relied on his memory of classified information | Released |
| | Pelton, Ronald | Relied on his memory of classified information | Life in prison |
| | Buchanan, Edward | Claimed access to classified information | 2 years and 6 months in prison |
| | Irene, Dale | Had accomplice with classified access | 2 years in prison |
| | King, Donald | Had accomplice with classified access | 30 years in prison |
| | Tobias, Bruce | Had accomplice with classified access | 5 months in prison |
| | Chiu, Rebecca | Had accomplice with classified access | 3 years in prison, renounce U.S. citizenship and deportation |
| | Pizzo, Francis | Had accomplice with classified access | 10 years in prison |
| | Pollard, Anne | Had accomplice with classified access | 5 years in prison |
| | Mortati, Thomas | Had accomplice with classified access | 1 year and 8 months in prison |
| | Alvarez, Elsa | Passed unclassified information | 3 years in prison and 1 year of probation |
| | Ali, Amen | Had accomplice with classified access | 5 years in prison and 3 years of probation |
| | Myers, Gwendolyn | Had accomplice with classified access | 7 years in prison and forfeiture of spouse's government salary and their sailboat |
| 1990s | Ames, Rosario | Had accomplice with classified access | 5 years in prison |
| | Brown, Joseph | Had accomplice with classified access | 6 years in prison |
| | Leung, Katrina | Had accomplice with classified access | Released as a result of prosecutorial misconduct |
| | Yai, John | Passed unclassified information | 2 years in prison and $20,000 fine |
| | Guerrero, Antonio | Passed unclassified information | Life in prison |

| Decade Began Espionage | Name | Method of Access or Type of Information in the Case | Outcome or Sentence |
|---|---|---|---|
| | Hernandez, Linda | Passed unclassified information | 7 years in prison |
| | Hernandez, Nilo | Passed unclassified information | 7 years in prison |
| | Santos, Joseph | Passed unclassified information | 4 years in prison |
| | Alonso, Alejandro | Passed unclassified information | 7 years in prison |
| | Groat, Douglas | Relied on his memory of classified information | 5 years in prison and 3 years of probation |
| | Sombolay, Albert | Passed restricted, but not classified information | 34 years in prison |
| | Charlton, Jeffrey | Retained classified information to sell after he lost his access | 2 years in prison, 5 years of probation, and $50,000 fine |
| | Latchin, Sami | Passed unclassified information | 4 years in prison |
| | Gari, George | Passed unclassified information | 7 years in prison |
| 2000s | Shaaban, Shaaban | Claimed access to classified information | 13 years in prison |
| | Smith, Timothy | Stole classified information | 3 years and 10 months in prison |
| | Kuo, Tai-Shen | Has accomplice with classified access | 15 years and 6 months in prison |
| | Nicholson, Nathaniel | Relied on accomplice's memory of classified information | 5 years of probation and 100 hours of community service |
| | Roth, John | Passed restricted, but not classified information | 4 years in prison and 2 years of probation |
| | Sherman, Daniel | Passed restricted, but not classified information | 1 year and 2 months in prison |
| | Shemami, Najeb | Passed unclassified information | 3 years and 10 months in prison |
| | Shu, Quan-Sheng | Passed restricted, but not classified information | 4 years and 3 months in prison and $387,000 fine |
| | Shriver, Glenn | Passed unclassified information | 4 years in prison |
| | Knapp, Marc | Passed restricted, but not classified information | 3 years and 10 months in prison |
| | Nozette, Stephen | Relied on his memory of classified information | 13 years in prison |

| Decade Began Espionage | Name | Method of Access or Type of Information in the Case | Outcome or Sentence |
|---|---|---|---|
| | Soueid, Mohamad | Passed unclassified information | 1 year and 6 months in prison |
| | Hoffman, II, Robert | Relied on his memory of classified information | 30 years in prison |
| | Kiriakou, James | Relied on his memory of classified information | 2 years and 6 months in prison |
| | Orr, Brian | Retained classified information to sell after he lost his access | 3 years and 1 month in prison, 3 years of probation, and $10,000 fine |

There are eight methods of access listed in Table 4, two more than were reported in the 2008 version of this report. Table 5 summarizes the frequencies of these eight methods.

**Table 5**
**Frequency of Methods of Access for Espionage Offenders with No Current Security Clearance**

| Method of Access or Type of Information in the Case | n=62 | % |
|---|---|---|
| Had accomplice with classified access | 21 | 34 |
| Passed unclassified information | 16 | 26 |
| Relied on memory of classified information | 10 | 16 |
| Stole classified information | 5 | 8 |
| Passed restricted, but unclassified information | 5 | 8 |
| Claimed access to classified information | 2 | 3 |
| Retained classified information to sell after losing access | 2 | 3 |
| Relied on accomplice's memory of classified information | 1 | 2 |

The most frequent method of obtaining information by persons who did not have access themselves was to rely on an accomplice. More than one-third of offenders, 34%, were accomplices to someone with active access to classified information. One additional person served as an accomplice to someone who relied on his memories of past access in order to pass classified information.

For example, Gwendolyn Myers was an accomplice and active participant in the espionage career of her husband, Walter Kendall Myers. Starting in 1978, the Myerses spied for Cuba for 30 years. They met in mid-life after matching failed marriages, a car accident in which Kendall Myers killed a teenaged girl, a disillusion with American politics, and a taste for radicalism that led them to grow marijuana in their basement and take illegal trips to Cuba. A Cuban intelligence official recruited them to serve as clandestine agents, and directed Kendall to seek employment in the Washington, DC, area that would provide classified access, such as at the Central Intelligence Agency (CIA) or DoS. In 1985, he moved from contract teaching at DoS and at the Johns Hopkins School of Advanced International

Studies—the same school Marta Velazquez and Ana Montes were then attending—to become a DoS professor and European analyst with Secret and later TS-SCI clearance. Gwendolyn worked in various jobs at a bookstore and also as an administrative assistant in a Washington, DC, bank, and never had classified access (Chaddock, 2009; Harnden, 2009).

Kendall and Gwendolyn were discreet, careful, and effective as agents for Cuba for 3 decades. He would memorize information at work or take notes to bring home overnight. Occasionally, he brought home classified documents that she would transcribe and he would return the next morning. They received encrypted radio broadcasts over a shortwave radio—the same model the Cubans provided to Montes—with directions, codes, and requests from their handlers. The Myerses preferred to hand papers directly to Cuban agents, so Gwendolyn would leave papers in her shopping cart and exchange the cart with an agent in the local supermarket. Over the years, they also met Cubans in various foreign locations including Mexico, Trinidad and Tobago, Argentina, Brazil, Ecuador, and Jamaica. Later, their handlers trained them in sending and receiving encrypted email from Internet cafes (United States District Court for the District of Columbia, 2009; Clark, 2010; Gentile, 2009).

The FBI began searching for a spy at DoS in 2006, and after Kendall made some intemperate public remarks that earned him criticism, he retired under a cloud in 2007. Focusing on the Myerses first by monitoring their emails and phone calls, the FBI set up a sting in which an undercover agent posed as a Cuban sent to reengage them. "I was actually thinking it would be fun to get back in to it," Kendall told the undercover agent in one of their meetings. Kendall and Gwendolyn Myers were arrested on June 4, 2009, and pled guilty in November of that year to acting as Cuban agents, conspiring to and actually collecting and transmitting national defense information to a foreign power, and wire fraud. Kendall was sentenced to life in prison without parole on July 16, 2010, and negotiated a lighter sentence for his wife in exchange for cooperating with extensive FBI debriefings. Gwendolyn received 6 and ½ years in prison, minus the time served since their arrest, which reduced her sentence to 5 and ½ years. He was 73 and she was 72 when they entered prison (United States Department of Justice, 2010; Hsu, 2010).

The judge noted at their sentencing that the Myerses were unrepentant and seemed serenely resigned. Kendall came from wealth and status in American society; he was the great-grandson of Alexander Graham Bell, and had attended exclusive private schools all his life. The couple lived in a luxury co-op on Cathedral Avenue in Northwest Washington, DC. They could afford to buy a small yacht and learned to sail in hopes that someday they could sail to Cuba. Early in their marriage, they fell in love with the Cuban revolution and with Fidel Castro. Castro granted them a personal audience in 1995 while they were visiting Cuba, and they received a medal from him for their espionage. They took no payment for their activities, motivated instead by their ideological commitment to Communism and Castro, and by the mutual adventure of being spies. "We share the ideals and dreams of the Cuban

revolution," they declared as they were sentenced to prison (Thompson, 2009; Harnden, 2009).

Nathaniel (Nathan) Nicholson is the one person who became an accomplice to espionage by relying on the memories of classified information recalled long after access had ended. The source was his father, Harold James (Jim) Nicholson. Jim Nicholson was already serving a prison sentence for his own espionage for the Soviets. He had been a career CIA officer starting in the 1980s; he became a station chief and a valued trainer of young CIA agents. Blaming a bitter and costly divorce, he began selling classified information to the Russians in June 1994, and continued until his unmasking and arrest in November 1996. He gave the Russians the names and assignments of all CIA trainees he had ever worked with, compromising and endangering them. He failed to pass a routine polygraph test in October 1995, which prompted surveillance and an investigation into his travel and finances (Joint CIA-FBI press release, 1996). Convicted of conspiracy to commit espionage in 1997, for which he received over $300,000, Jim Nicholson began serving a 23 and ½ year prison sentence at the Federal Correctional Institution in Sheridan, Oregon, not far from where his three children were to live with his parents during his incarceration. His youngest son, Nathan, was 12 (United States Department of Justice, 2009).

Jim Nicholson did not give up. Though the authorities monitored his communications in prison, the FBI noted in 2002 that Nicholson was trying to manipulate fellow inmates into contacting the Russians for him. When Nathan returned to Portland from serving as a paratrooper in the Army Rangers in 2006 with an injury that put him out of the military, Jim began grooming his son to be his go-between with the Russians. Jim claimed the Russians owed him a "pension" they had promised, and he wanted them to pay before any information he still had in his head went stale (Lichtblau, 2009).

Nathan, then 22, visited his father regularly in prison during 2006, receiving training and advice on how to contact and establish a connection with the Russians, how to travel to meeting places without attracting attention, how to carry cash payments into the country, and how to bank the money surreptitiously. Jim wrote out notes and questions for the Russians that Nathan smuggled out of the prison on crumpled paper. Nathan began a 2-year odyssey meeting Russian handlers in various world cities, including San Francisco, Mexico City, Lima, and Nicosia. The Russians proved interested in renewing this contact, and pressed Jim Nicholson for details from the mid-1990s about how he thought he might have been caught. They hoped to do their own damage assessment to find a possible mole in Russian intelligence who could have betrayed Nicholson. Jim passed on through Nathan details of his last months as a Russian agent, including his suspicion that a contact in Malaysia had been tainted, the name of the CIA polygraph examiner who failed him, descriptions of federal agents who interrogated him after his arrest, concerns that he had been tailed while working as deputy station chief in Malaysia,

and suspicion that his computer at the CIA training facility had been tapped (Denson, 2010).

Nathan collected $47,000 in installments from the Russians, which at Jim's direction, he disbursed among his family members. Nathan was exhilarated by this secret adventure, but in fact, it was no secret. The FBI got court approval to tap Nathan's cell phone, intercept his email, search and surveil his apartment, and track his vehicle. FBI agents followed him on all of his travels and, when he returned from Nicosia, Cyprus, they detained him while they searched his luggage and photocopied his spy notebook with the codes, addresses, questions, and notes he used, plus a $7,000 payment hidden in a video game case (Pincus, 2010). Nathan was arrested in January 2009, pled guilty to acting as a foreign agent and to money laundering, and, after his father also pled guilty so that his son would not have to testify against him, they appeared at a joint sentencing hearing in January 2011. Nathan was sentenced to 100 hours of community service with his fellow military veterans and 5 years of probation. Jim Nicholson received 8 years in prison added onto his existing sentence. He will be in his early 70s upon his release in 2024 from a federal prison in Terre Haute, Indiana, far from his family in Oregon (Pincus, 2010; Denson, 2011).

Gwendolyn Myers and Nathaniel Nicholson are examples of persons who became accomplices to other people who had active access to classified information or, in Nicholson's case, relied on the memories of another's past access. Combined, these two categories based on the role of accomplices account for 36% of methods used by persons with no clearance themselves, and makes being an accomplice the most frequent among non-clearance holders.

The second most frequent method of committing an espionage-related offense without having a security clearance is to pass unclassified information. This may seem counterintuitive: how does the transmittal of unclassified information result in an espionage-related conviction? U.S. espionage statutes do not consistently require the information to be classified. The laws have built on one another over time, becoming complex and contradictory. Early major statutes specify "national defense" information because they were written before classification was even developed early in the Second World War; only later statutes starting in 1950 specify classified information (Edgar & Schmidt, Jr., 1973; Elsea, 2013).

John Joungwoong Yai is an example of someone who had no access to classified information himself, but who passed unclassified information to a foreign nation and was convicted of an espionage-related offense. A naturalized citizen since 1981, Yai was a successful businessman who owned and operated various small businesses in Los Angeles. He was arrested early in 2003 after a 7-year FBI investigation that used wiretaps, electronic surveillance, and secret searches. For at least 3 years, Yai sent his contact in North Korea publicly available information about trends in U.S. government intentions toward North Korea. He also plotted to get access to classified information for himself by getting a government job, and

worked to plant other young Koreans in jobs that would have access to classified information so they could serve as his collectors. Yai communicated with and took taskings from his North Korean handlers via coded messages sent by fax and email, and also during meetings in Europe, China, and North Korea. He was paid at least $18,000 for his efforts. He pled guilty to acting as an agent of a foreign power and to several counts of customs violations for his failure to declare his earnings over $10,000 upon reentry into the U.S. after his meetings. Yai's wife, Susan Younja Yai, accompanied him on trips to meet with his North Korean handlers, and as a result, she received a year of probation and $500 fine. In February 2003, Yai was sentenced to 2 years in prison (Krikorian, 2003; Federal Bureau of Investigation, Affidavit, 2003; United States District Court for the Central District of California, Indictment, 2002).

The third-most frequent method of committing an espionage-related offense without having personal access to classified information was to rely on one's memory of classified information after losing access. Ten individuals called up information from their memories and then sold or gave it to persons unauthorized to receive it. Robert Hoffman, II is a recent example.

After 20 years in the U.S. Navy, Hoffman retired in November 2011 as a Petty Officer First Class (E-6) rated as a Cryptologic Technician-Technical. His work with electronic sensors used in submarine surveillance and tactical guidance to the commander meant that he had held access to highly classified information. A few months before his retirement, he traveled to the Republic of Belarus, ostensibly in search of several Byelorussian women he had enjoyed meeting earlier during a port call in Bahrain. He posted descriptions of his 3-week trip on social media, including the unlikely boast that he had dropped in on the President of Belarus. The FBI began to follow him, and a female undercover agent answered Hoffman's Craigslist ad seeking companionship. She conducted a 5-month courtship over the Internet and met him for several dates (United States Attorney's Office Eastern District of Virginia, 2014; Daugherty, 2013a; Daugherty, 2014).

Then, the FBI raised the stakes and sent Hoffman a letter, apparently from "Vladimir" in Russia, inviting him to help with technical expertise for which he would be well-compensated. Within hours, Hoffman agreed to this proposal and volunteered his help. In his diary and in later statements, he said he needed money, but also that he liked the thrills espionage promised. Over several months, he delivered three collections of classified information on thumb drives to a hollow at the base of a tree in First Landings State Park in Virginia Beach, the dead drop site suggested by the FBI. The information Hoffman left in the tree covered naval capabilities and equipment, specific missions, and data about adversaries and intelligence, which would have allowed the Russians to track American submarines while avoiding detection. According to the Assistant U.S. Attorney speaking at Hoffman's trial, "He did not pass official government documents but instead created his own documents of secret information from memory" (McGlone, 2012). The FBI arrested Hoffman early in December 2012. He was convicted of attempted

espionage at trial in August 2013, and sentenced on February 10, 2014, to 30 years in prison (Federal Bureau of Investigation, 2014; Daugherty, 2013b).

Five of the persons convicted of espionage-related offenses who did not hold security clearances or access to classified information passed information or technology that was restricted because, as a military defense or dual military and commercial use, it was subject to export control laws. Export in this context includes the sharing of information (Title 22 U.S.C. chapter 39, § 2778). Marc Knapp is a recent example of someone in this group who tried to export restricted military technology to a hostile foreign power under a trade embargo.[8]

Starting in December 2009, for 7 months Knapp negotiated with a person he thought was a buyer for Iranians seeking export controlled American military equipment and manuals. Knapp collected military hardware, so he had connections into the world of buying and selling such articles. He also needed money. He had been unemployed since 2007 after he lost his human resources job at a biotechnology company (Associated Press, 2011; O'Sullivan, 2011). An acquaintance of Knapp's, who was already being investigated for illegal technology export, pointed investigators to Knapp as one of the sources of the equipment he had sold, and cut a deal for a light sentence in exchange for cooperating against Knapp. The buyer was actually an undercover agent from the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (Department of Justice, 2011).

Knapp promised the undercover agent he could deliver multiple anti-gravity flight suits, an F-14 NATOPS emergency procedures manual for use in flight emergencies in various U.S. military aircraft, multiple electronic versions of this manual, four AN/PRC-149 survival radios, two F-14 aircraft pilot ejection seats and, most dramatically, an F-5B Tiger II fighter jet aircraft offered at $3.25 million (Department of Justice, 2011). The agent documented Knapp explaining to him that prohibited customers for such sensitive U.S. military hardware, including Iran and, he hoped, China and Russia, could benefit by reverse engineering these technologies, or they could choose to "just listen in" to emergency beacon signals coming from downed American pilots (Immigration and Customs Enforcement, 2011). He saw himself "leveling the playing field" for his customers vis-à-vis the more advanced position of the U.S. (United States District Court for the District of Delaware, 2010).

Knapp insisted he and the agent use code words and false names to discuss their plans. He opened an offshore bank account to store his commission, and he used

[8] Knapp was charged with one count of violating the International Emergency Economic Powers Act, Title 50, U.S.C. § 1702 and 1705(c), and Executive Order 13222, and Title 31 C.F.R. § 560.204-560.205, and one count of violating the Arms Export Control Act, Title 22 U.S.C. § 2778(b)(2) and 2778(c), and Title 22 C.F.R. § 121.1, 123.1, and 127.1. Punishments for violating arms control export laws can be harsh: Knapp faced a possible maximum statutory sentence of 30 years incarceration, followed by 3 years supervised release, a $2,000,000 fine, forfeiture, and a $200 mandatory special assessment.

only encrypted email. He grasped the complicated procedures and paperwork required to export something as sensitive and obvious as a jet fighter plane, and realized how to lie at the right times in order to proceed. He delivered several shipments of the smaller equipment to Hungary, his transshipment point to Iran. Once on the ground in Hungary, the shipments were swiftly collected by ICE. Knapp was making his final arrangements to have the fighter jet flown to the east coast for crating when the Department of Homeland Security (DHS) arrested him on July 20, 2010. He pled guilty the following July and was sentenced in September 2011 to 46 months (3 years and 10 months) in prison (Immigration and Customs Enforcement, 2011).

Another five individuals without access to classified information simply stole it. One of the "year of the spy" offenders from 1985, Randy Jeffries, took advantage of his employer's lax security routines and took classified materials to try to sell to the Soviets.

Jeffries worked as a messenger for the Acme Reporting Company in Washington, DC, a stenographic reporting service contracted to federal agencies and Congressional committees. Minutes, notes, documents, and testimony, all on paper and some of it classified Secret or TS, would be picked up by messenger and brought to Acme to be transcribed, photocopied, and routed for publication or storage. Jeffries had worked in his low-paid, routine job for 2 months. He had no security clearance, since he was coming back from several years of drug rehabilitation after he lost an FBI clerk's job, where he had held a clearance (Department of Defense Security Institute, 1990).

Jeffries set aside a stack of classified pages of testimony while he was working on destroying piles of papers by tearing them into four pieces and stuffing them into plastic bags and then into a dumpster available to all in an alley.[9] Jeffries then took the pile of classified pages home with him and called the Soviet Military Office, saying he was coming to speak with them. The FBI noted his arrival and his visit, and then a second visit. They called Jeffries posing as Soviets, and offered to meet in a hotel to discuss an arrangement. Jeffries told the undercover agents that he already had given over 40 pages of samples, had not yet been paid, and asked for $5,000. The FBI arrested him. He pled guilty to passing national defense information to a person not entitled to receive it and was sentenced in March 1986 to between 3 and 9 years in prison (Department of Defense Security Institute, 1990; Dolan, 1986).

The last two of the eight categories of persons convicted of espionage-related offenses without holding a security clearance or access to classified information each have only two instances. Edward Buchanan and Shabaan Shabaan claimed to

[9] Part of the impact of this case came from learning about the egregious security environment the Acme Reporting Company had maintained by lying about its procedures as a cleared industrial security facility to Defense Investigative Service (DIS) auditors. DIS revised its audit procedures as a result of these revelations.

potential buyers that they had access to classified information they wished to sell, but, in fact, neither one did. While still a student in Air Force training in 1985, Buchanan offered the East Germans and the Soviets classified information for sale. Air Force Office of Special Investigations agents conducted a sting, and learned that, as a student, Buchanan had no classified documents, but he did have plans to commit espionage as soon as his TS-SCI clearance, then in process, came through. He was court-martialed and sentenced to 30 months of confinement (Crawford, 1998).

Shabaan, a naturalized U.S citizen originally from Palestine, traveled to Iraq before the 2003 U.S. invasion and offered to provide Iraqi intelligence with the names of all American spies operating in Iraq, which he falsely claimed he could procure from his classified sources. He also offered them a band of sympathizers he claimed he could organize as human shields against the coming invaders (Federal Bureau of Investigation, 2006). He was convicted at trial of acting as an agent of a foreign power without notifying the Attorney General as required by law, violating the economic sanctions against Iraq, fraudulently procuring U.S. citizenship, and tampering with a witness (he threatened to behead the person, his brother). In May 2006, Shabaan was sentenced to 160 months (13 years and 4 months) in prison (United States Department of Justice Southern District of Indiana, 2006; Corcoran, 2006).

Finally, Jeffrey Charlton and Brian Orr worked in jobs that required access to classified information and they held security clearances, but each stole documents shortly before losing their access. Charlton was an engineer at Lockheed Corporation in the 1980s and retired early in 1989, but he was disgruntled over the retirement terms offered and took with him a cache of classified documents relating to U.S. Navy stealth and anti-submarine programs. In an FBI sting, on five occasions Charlton offered to sell these documents for $100,000. He was arrested, pled guilty, and was sentenced in April 1996 to 2 years in prison, 5 years of supervised release, and fined $50,000 (Chu, 1996).

Brian Scott Orr worked as a civilian computer engineer at the U.S. Air Force Research Laboratory in Rome, New York, between 2009 and 2011. He held a TS clearance in order to work on the Air Force Satellite Control Network, the computer network that controls military satellites. Orr's access was withdrawn in 2011 and he reacted by retiring, taking with him training course materials for the computer network and sensitive technical data that could have allowed someone to seriously disrupt or destroy the military satellite system. Orr negotiated a deal with an FBI undercover agent he thought was a representative of the PRC, and sold two thumb drives' worth of data for $5,000. He was arrested and pled guilty in March 2014 to retention of stolen government property. He was sentenced in September 2014 to 37 months in prison (3 years and 1 month), 3 years of supervised release, and fined $10,000 (Federal Bureau of Investigation Los Angeles Division, 2014).

The proportion of espionage-related offenders who did not hold current security clearances increased to almost half in the recent cohort—44%—in part because the variety of available espionage activities is proliferating.[10] It is inaccurate to assume that espionage-related offenses have been or only can be committed by security clearance holders, or that the information at issue would necessarily have been classified. The examples underline the fact that some persons who held no security clearance and/or had no current access to classified information have been convicted of espionage-related offenses because they relied on accomplices, memory, theft, lies, or unauthorized retention. The examples also illustrate that it is quite possible to be convicted of espionage–related offenses for collecting and passing unclassified information.

[9] Beginning in the 2008 report, espionage of types other than classic were discussed. For example, Ronald Hoffman's sale of dual-use technology produced under an Air Force contract was included. Since 2008, prosecutions for acting as an agent of a foreign government, leaks of classified information to the press, violations of export controls, and economic espionage have all increased notably, and so there is a higher proportion of such cases included in the PERSEREC Espionage Database in 2015.

## ELEMENTS OF THE ACT OF ESPIONAGE

Of the five sections in Part 1 of this study, four of them capture information about the 209 individuals themselves—their demographic characteristics, employment and clearance status, the consequences they suffered for their crimes, and their motivations. The focus of this section is different in that it reports details of what these individuals did to commit espionage and what kind of spies they were (i.e., did they volunteer, were they intercepted, and which country did they try to contact). By collecting data on basic dimensions of their acts of espionage, it may be possible to discern trends in how espionage has been conducted by Americans over time. Table 6 presents some of these basic dimensions.

**Table 6**
**Elements of the Act of Espionage**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=68* | *%* | *n=74* | *%* | *n=67* | *%* |
| Intercepted or passed information | | | | | | |
| Intercepted | 6 | 9 | 29 | 39 | 19 | 28 |
| Passed information | 62 | 91 | 45 | 61 | 48 | 72 |
| Duration | | | | | | |
| Intercepted | 6 | 9 | 29 | 39 | 19 | 28 |
| Less than 1 year | 14 | 20 | 10 | 13 | 14 | 21 |
| 1 to 4.9 years | 23 | 34 | 16 | 22 | 22 | 33 |
| 5 or more years | 25 | 37 | 19 | 26 | 12 | 18 |
| Volunteer or recruit | *n=67* | | | | *n=66* | |
| Volunteer | 34 | 51 | 47 | 64 | 39 | 59 |
| Recruit | 33 | 49 | 27 | 36 | 27 | 41 |
| Recruited by | *n=33* | | *n=27* | | *n=27* | |
| Family | 2 | 6 | 3 | 11 | 3 | 11 |
| Foreign intelligence | 26 | 79 | 15 | 56 | 16 | 59 |
| Friend | 5 | 15 | 9 | 33 | 8 | 30 |
| Method used to begin espionage | *n=66* | | *n=72* | | *n=56* | |
| Contact foreign agent | 9 | 14 | 10 | 14 | 1 | 2 |
| Contact foreign embassy | 17 | 26 | 28 | 39 | 13 | 23 |
| Go-between | 5 | 7 | 3 | 4 | 1 | 2 |
| Other methods | 2 | 3 | 3 | 4 | 8 | 14 |
| Internet | 0 | 0 | 1 | 1 | 6 | 11 |
| Recruited | 33 | 50 | 27 | 38 | 27 | 48 |
| Location where espionage began | *n=66* | | *n=73* | | | |
| Outside U.S. | 27 | 41 | 16 | 22 | 12 | 18 |
| U.S. east coast | 28 | 42 | 27 | 37 | 32 | 48 |
| U.S. west coast | 6 | 9 | 19 | 26 | 12 | 18 |
| Other locations in U.S. | 5 | 8 | 11 | 15 | 11 | 16 |
| Location where espionage began outside the U.S. | *n=27* | | *n=16* | | *n=12* | |
| Western Europe | 20 | 74 | 11 | 69 | 1 | 8 |
| Asia and Southeast Asia | 4 | 15 | 3 | 19 | 5 | 42 |
| Eastern Bloc/Soviet Union | 3 | 11 | 1 | 6 | 0 | 0 |
| Africa | 0 | 0 | 1 | 6 | 0 | 0 |
| Middle East | 0 | 0 | 0 | 0 | 3 | 25 |
| Central and South America | 0 | 0 | 0 | 0 | 3 | 25 |

**ELEMENTS OF THE ACT OF ESPIONAGE**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| Attempts and transmissions of information to recipients by region* | *n=69*** | | *n=80*** | | *n=77*** | |
| Western Europe | 2 | 3 | 1 | 1 | 4 | 5 |
| Soviet Union/Russia | 42 | 61 | 39 | 49 | 9 | 12 |
| Eastern Bloc | 15 | 22 | 14 | 17 | 1 | 1 |
| Asia and Southeast Asia | 4 | 6 | 10 | 13 | 22 | 29 |
| Africa | 1 | 1 | 2 | 3 | 0 | 0 |
| Middle East | 3 | 5 | 3 | 4 | 15 | 20 |
| Central or South America | 1 | 1 | 5 | 6 | 11 | 14 |
| Al Qaeda | 0 | 0 | 1 | 1 | 4 | 5 |
| USA (information revealed publicly) | 0 | 0 | 0 | 0 | 7 | 9 |
| Recipient unknown | 1 | 1 | 5 | 6 | 4 | 5 |

* For several individuals, it has not been revealed whether they contacted government officials or private businessmen in some of the countries they dealt with. In one instance, Noshir Gowadia, court documents show that he named multiple countries he had contacted and attempted or did pass information to, but the documents only list six countries by name, so two of the four attempts reported in the third cohort listed as "recipient unknown" are Gowadia's.
** Some individuals transmitted information to two or more recipients, so the number of instances of actual or attempted passing of information in this section of the table is greater than the number of individuals in each of the three groups.

Table 6 demonstrates that during the 3 decades of the first cohort, almost all—91%—transmitted information to a recipient. This success rate among American spies fell sharply during the 1980s when younger, enlisted military volunteers attempted and usually failed at espionage while trying to earn money (Herbig, 2008). The most recent cohort of offenders has passed information more often than the second cohort but less often than the first. Seventy-two percent of espionage offenders since 1990 have transmitted information, less than the 91% of the first cohort, but more than the 61% of the second cohort.

The duration of espionage careers reinforces the finding that the 1980s were an anomaly in the history of American espionage. Looking at the first two categories, intercepted before passing information and passing information for less than a year, 52% of American spies in the 1980s never got their spying started or were quickly caught. In comparison, less than one-third of offenders in the first cohort had such short careers. The most recent cohort shows fewer interceptions than during the 1980s (28% rather than 39%), but 21% of offenders were quickly caught within 1 year.

The pattern for offenders who spied between 1 year and 4.9 years echoes the impact of the 1980s: one-third of the first cohort had these mid-length espionage careers, while only 22% of the 1980s cohort did so, and again, one-third of the recent cohort spied between 1 year and 4.9 years.

In a heartening finding for counterespionage, the trend among long duration espionage careers is consistently downward. Among the first cohort, 37% spied for

5 or more years. In the second cohort, this fell to 26%, and in the most recent cohort, long duration espionage is down to 18%.

There always have been more volunteers to commit espionage than recruits among American spies, but the proportions have varied over time. The early cohort was roughly half volunteers and half recruits. During the 1980s, volunteers increased to 64% of the total. Fifty-nine percent of offenders since 1990 volunteered to commit espionage while 41% were recruited, making this cohort more volunteers than the first but less than the second.

Recruitment of American spies by a foreign intelligence service predominated among recruits in the first cohort during the early Cold War, with 79% of those recruited, followed by 15% recruited by a friend and only 6% by a family member. This proportion changed during the 1980s and has remained so since 1990. In the second cohort, foreign intelligence services recruited 56% of recruits, while the percentages recruited by family or friends each doubled when compared with the first group. The third cohort mirrors the second, with 59% recruited by a foreign intelligence service, 11% by a family member, and 30% by a friend.

Among the methods of first contact with a recipient by volunteer American spies, contacting the potential recipient's embassy is the most common. About one-quarter of volunteers telephoned or walked into embassies in the first cohort, as did 39% in the 1980s and 23% in the most recent cohort, even though it has been widely reported in the press that the FBI watches the entrances of embassies that would be likely recipients of information, such as that of the Soviet Union, and also attempts to place taps on their telephones and communications.

Another common method to try to begin espionage was contacting a foreign agent, which usually meant a nation's military intelligence officials or an attaché. A few offenders in each cohort worked through a go-between to an intelligence service.

As the Internet has become increasingly useful and convenient, more volunteer spies have electronically approached prospective recipients. In the most recent cohort, eight individuals used the Internet to make contact with recipients. Paul Hall, who took the name Hassan Abujihaad, is one example.

Paul Hall grew up in San Bernardino, California, and joined the U.S. Navy in 1995 when he was 19. He converted to Islam, changed his name to Hassan Abujihaad (Abujihaad means "father of holy war" in Arabic) and, around the time of the Al Qaeda bombing of the *U.S.S. Cole* in October 2000, began an email correspondence with a London-based English language Islamist website run by Azzam Publications. Six years later, in March 2007, he was arrested and charged with materially aiding terrorism with intent to kill U.S. citizens and transmitting classified information to those not authorized to receive it (Medina, 2007). In February 2008, Abujihaad stood trial and was convicted on both charges ("Former sailor," 2008).

Abujihaad allegedly contacted the Azzam Publications website late in 2000 to order videos that encouraged violent jihad. From his military duty station as a signalman on the destroyer *U.S.S. Benfield*, he ordered several videos and corresponded by email about payment and shipment options. He also reached out to anonymous jihadists at the website to express his enthusiasm for his adopted faith and for terrorist tactics. Referring to the Islamist fighters in one of his videos, he wrote,

> with their only mission in life to make Allah's name and mission supreme all over the world, I want to let it be known that I have been in the middle east [sic] for almost a total of 3 months [that is, while onboard *the U.S.S. Benfield*]. For those 3 months you can truly see the effect of this psychological warfare [from the attack on the *U.S.S. Cole*] taking a toll on junior and high ranking officers...[they were] running around like headless chickens very afraid. (United States District Court for the District of Connecticut, Warrant, 2007)

Authorities stumbled on Abujihaad by following links from two other terrorism arrests, one of which was in London. In 2004, the founder of the Azzam Publications website, Babar Ahmad, a British national of Pakistani descent, and his colleague, Syed Talha Ahsan, were indicted in the U.S. and arrested in London for allegedly providing material support to Chechen terrorist groups and the Taliban by running a network of fundraising websites that served as a "recruitment and propaganda tool for al Qaeda and the mujahedeen" (Thomas, Ryan & Date, 2007). The indictments against Ahmad and Ahsan had been filed in U.S. District Court in Hartford, Connecticut, the site of one of the website's Internet service providers. The two website owners fought extradition to the U.S. in the British courts starting in 2004 (Whitlock, 2005; Associated Press, 2012). Shortly before their arrest, a raid on Ahmad's house turned up a password-protected floppy disk with the plan for a U.S. Navy battle group (including the U.S.S. *Benfield*) to transit from California to

the Persian Gulf in the spring of 2001.[11] The material on the disk also pointed out vulnerabilities in the ships' defenses and the best locations from which to attack the fleet. Prosecutors alleged this classified information was sent by Abujihaad, who held a Secret clearance and was passing it along to his friends at Azzam Publications (United States District Court for the District of Connecticut, Warrant, 2007; United States Attorney's Office District of Connecticut, 2007).

The second link that led to Abujihaad was from a terrorism arrest in the greater Chicago area. Abujihaad left the Navy in 2002 with an honorable discharge. In the fall of 2004, he was in Phoenix, Arizona, rooming with a fellow would-be jihadist, Derrick Shareef, when news broke that Babar Ahmad had been arrested in London and the Azzam website had been shut down. Shareef, in turn, was arrested early in December 2006 in Genoa, Illinois, where he was accused of planning a terror attack on holiday shoppers at the CherryVale shopping mall. He had bartered his stereo speakers for hand grenades that were actually duds in an FBI sting operation (White, 2007). While under arrest, Shareef reported to investigators that two years earlier, his roommate, Abujihaad, had been upset when he learned about Ahmad's arrest. He had blurted out, "I think this is about me", started to cry, and soon set about destroying his videos and deleting his emails from Azzam Publications. This information, added to the evidence of the classified fleet transit plan and the emails that had been exchanged with Azzam personnel, led to Abujihaad's arrest in Phoenix in March 2007. At the time, Abujihaad was working for UPS as a deliveryman and supporting two small children (White, 2007).

Abujihaad was convicted on March 6, 2008, of providing material support to terrorists and of disclosing classified information related to the national defense to those unauthorized to receive it. A year later, a judge granted a defense motion for

---

[11] The case of Babar Ahmad is outside the scope of this study since Ahmad is a British citizen, but it illustrates the potential for linkages between espionage and terrorism. Ahmad founded Azzam.com in 1996 as the first English language jihadist website, setting the standard for all subsequent global sites that sought to communicate in English, and for the first time linking to established sites in Arabic, making them accessible to a larger audience. He featured sophisticated graphics on his site, and he advanced a radical agenda in a tone of moderation, luring in the curious and gullible. "It taught an entire generation about jihad," one terrorism researcher noted. "Even in its nascency, it was professional." Since his arrest in 2004, Ahmad worked from prison to publicize his plight and to advance the Islamist cause to a wider audience. Working with relatives and friends outside who put his material onto his new website, Ahmad argued that if he were extradited to Connecticut, he would end up a casualty of the U.S. war on terror, and imprisoned in Guantanamo Bay. British public figures, antiwar activists, Muslim support groups, and entertainment notables came out in support of Ahmad in his claim of innocence. Ten thousand people signed an online petition calling on the British government to block the extradition, and 140,000 people signed another in 2012. In 2005, Ahmad ran for Parliament from his cell, garnering 2% of the vote in his district (Whitlock, 2005). He won £60,000 in damages for injuries he received from the police during their raid on his apartment and his initial arrest. Extradited to the United States in 2012, he pled guilty in December 2013 to providing material support to terrorists, and was sentenced in July 2014 to 12 and ½ years in prison. Since he had already been held in 10 different jails and prisons either in the U.K. or in the U.S. for over 11 years, many in solitary confinement, he was released to return to the UK in July 2015. He maintains that although the classified battle plan was found in his apartment, he never did anything with it or passed it to anyone else (Kundnani & Theoharis, 2014; Ratcliffe, 2015).

his acquittal on the charge of providing material support to terrorists based on the judge's application of the law's language. On April 3, 2009, Abujihaad was sentenced to 120 months (10 years) in prison on the remaining charge of disclosing classified information about the battle group plan of transit to the publishers of the Azzam website, Ahmad, and Ahsan (U.S. Department of Justice Press Release, 2009; Mahony, 2009).

The remaining six persons in the most recent cohort used various methods to contact recipients, including in-person meetings, sending offers through the mail, and, in one instance, granting foreign nationals who worked in a laboratory access to export restricted materials.

John Reece Roth, a 72-year-old University of Tennessee emeritus physics professor and expert in plasma technology, headed a lab researching plasma actuators for drones as a subcontractor to Atmospheric Glow Technology, Inc. Despite being warned that he was violating the law, Roth insisted on including promising foreign graduate students, one from China and the other from Iran, on the research, even though the contract specified that any technology to be developed was export controlled and could not be shared with foreign nationals. Roth also sent documents based on the research via email to professional contacts in China, and took other documents with him to China to present in person. He was charged with conspiring with the company to defraud the Air Force, 15 counts of violating the Arms Control Export Act, and one count of wire fraud. Convicted on all counts on September 3, 2008, Roth was sentenced in July 2009 to 48 months in prison (4 years) followed by 2 years of supervised release (Satterfield, 2008; United States Department of Justice, 2008; United States Department of Justice, 2009).

Offenders in the first cohort in Table 6 were most likely to begin their espionage either overseas (41%) or on the east coast of the U.S., where government agencies and intelligence headquarters are concentrated. There has been a steady decline over time in the proportion of espionage cases begun overseas, such that in the recent cohort, only 18% began outside the U.S., and roughly half originated on the east coast. The remainder was divided between the west coast and other U.S. locations.

Looking specifically at the small numbers of individuals who began espionage overseas and in what region of the world these persons were physically located when they first acted, there is a large shift between the first two cohorts and third. In the first two cohorts, most overseas cases began in Western Europe, in the Eastern Bloc, or in the Soviet Union. In a few cases, they began in Asia or Southeast Asia.[12] In the most recent cohort, only one case has been initiated in Western Europe, five in Asia or Southeast Asia, and three each in the Middle East,

[12] This variable reports the location of initial contact, but not the nationality of the recipient. Many instances that occurred in Western Europe involved Americans interacting with Soviet or Eastern European contacts.

Central, or South America. Americans looking to commit espionage appear to have spread around the globe as customers for their information have expanded.

The shift in recipients coincided with the collapse of the Soviet Union in 1991. Eighty-three percent of the attempts or actual transmissions by individuals in the early Cold War cohort went to the Soviet Union or to the Eastern Bloc countries, which sent them as a matter of course to the Soviets. Soviet predominance as the recipient for American espionage also remained high in the later Cold War decade of the 1980s, with 66% of attempts or transmissions to the Soviet Union or to the Eastern Bloc. In the third cohort, the Soviet Union or Russia and the Eastern Bloc nations declined as recipients to only 13% of attempts or transmissions.

Only a few Western European nations received the fruits of American espionage in each of the three cohorts; the most recent cohort is the largest with four Western European recipients. Countries in Asia and Southeast Asia, predominantly China, have become more common recipients of American espionage, with the percentages of attempts or transmissions increasing from 6% in the first cohort to 13% in the second to 29% since 1990. The Middle East and the countries of Central and South America likewise grew in popularity as recipients: from 5% and 4% in the first two cohorts, the Middle East increased to 20% of attempts or transmissions, while Central and South America increased from 1% to 6% to 14% since 1990. Finally, Al Qaeda served as the recipient in four instances since 1990, and in seven instances, Americans attempted or transmitted information to other Americans, usually journalists or public news sources, which then resent the information out into the world.

A chart of these data on recipients of espionage by Americans in Figure 1 illustrates the prevalence of the Soviet Union and their Eastern European allies during the first two periods, and the shift to a greater variety of recipients in the recent cohort.

ELEMENTS OF THE ACT OF ESPIONAGE

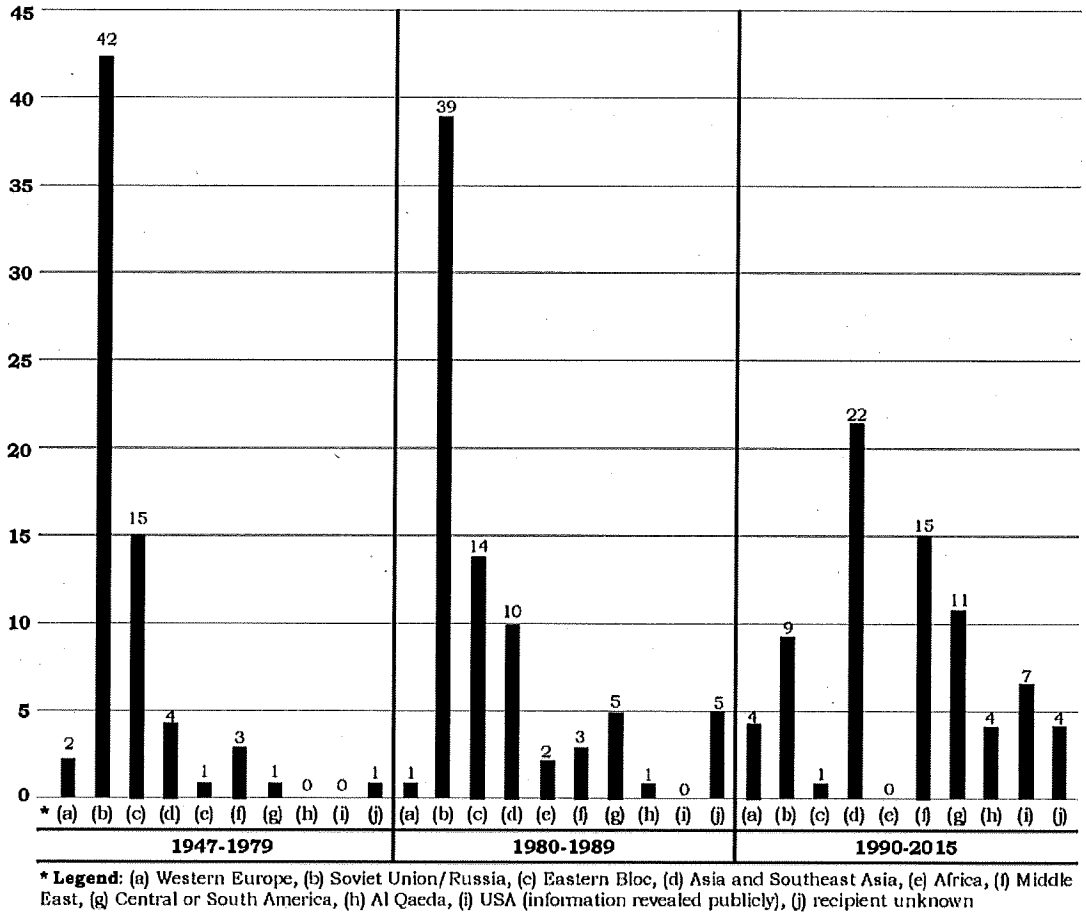



**Figure 1 Number of Attempts and Transmissions of Information to Recipients, by Region**[13]

The more equal opportunity competition for American secrets among recipients since 1990 implies more challenges for American counterespionage, since there are several foreign intelligence services to counteract and more foreign interests to watch. The Russians continue their traditional espionage activities, China invests heavily in its distinctive information gathering efforts, and Cuba fields effective intelligence service activities inside the U.S. The three largest recipient countries for American espionage in the recent cohort since 1990 are China (15), the Soviet Union or Russia (nine), and Cuba (seven). However, there also are a larger number of recipients of even one or two instances of offers from Americans, including Cambodia, Iraq, Iran, Israel, Syria, Taiwan, Venezuela, France, South Korea, and Saudi Arabia. Approaches to these countries were not uniformly welcomed or accepted.

[13] This graph includes both attempts and completed transmissions of information.

### How Information Has Been Transmitted

Table 7 reports on three variables related to information transmittal during espionage-related acts: the media in which the information was prepared for transmittal; the method that was used to transmit it; and the location of the spy when the information was transmitted. These variables sometimes reflect knowledge that was gained by counterintelligence or law enforcement officers in the course of their investigations, and since they may reveal the sources or methods that were used, such information is often withheld or vaguely described in open sources. As such, there are much missing data in these variables. Even if an entry is coded "no" (i.e., there is no mention in open sources of its use in the case), one cannot be certain that it was not used, only that it was not revealed publicly. Therefore, these variables are not reported for each individual because we cannot know for sure that additional methods were not also used. Instead, all entries for each variable are reported in the three cohorts as choices, and the sum of those reported methods is then used to derive the percentages listed by entry within a cohort.

**Table 7**
**What, How, and Where Information Was Transmitted**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| Media transmittal choices | *n= 73 choices* | *% of 73* | *n= 91 choices* | *% of 91* | *n= 106 choices* | *% of 106* |
| Original documents or photos | 37 | 51 | 39 | 43 | 32 | 30 |
| Photos, films, or videos of originals | 16 | 22 | 13 | 14 | 5 | 5 |
| Photocopies | 8 | 11 | 9 | 10 | 14 | 13 |
| Parts or equipment | 0 | 0 | 4 | 4 | 3 | 3 |
| Microfiche or via short wave radio | 6 | 8 | 5 | 5 | 7 | 7 |
| Memory | 4 | 5 | 11 | 13 | 15 | 14 |
| Electronic files | 2 | 3 | 10 | 11 | 30 | 28 |
| Method transmittal choices | *n= 73 choices* | *% of 73* | *n= 102 choices* | *% of 102* | *n= 77 choices* | *% of 77* |
| Meeting in person | 46 | 63 | 35 | 34 | 44 | 57 |
| Courier | 10 | 14 | 13 | 13 | 3 | 4 |
| Telephone | 2 | 2 | 11 | 11 | 11 | 14 |
| Dead drop | 7 | 10 | 5 | 5 | 5 | 6 |
| Mail or telegram | 7 | 10 | 11 | 11 | 7 | 9 |
| Not attempted | 1 | 1 | 27 | 26 | 7 | 9 |
| Location transmittal choices | *n= 49 choices* | *% of 49* | *n= 76 choices* | *% of 76* | *n= 80 choices* | *% of 80* |
| Out of country | 25 | 51 | 22 | 29 | 25 | 31 |
| Out of town from residence | 6 | 12 | 9 | 12 | 11 | 14 |
| Hotel or motel room | 0 | 0 | 0 | 0 | 10 | 13 |
| P.O. box | 0 | 0 | 1 | 1 | 3 | 3 |
| Embassy | 7 | 15 | 8 | 11 | 8 | 10 |
| Parking lot | 2 | 4 | 1 | 1 | 1 | 1 |
| Not attempted | 6 | 12 | 27 | 35 | 3 | 4 |
| Other | 3 | 6 | 8 | 11 | 19 | 23 |

Among the types of media transmitted by the persons in the first cohort, half were original documents. This declined in the second cohort to 43% and then to 30% in the third cohort as photocopying and electronic transmission grew common starting in the 1980s. Taking photographs or filming original documents comprised almost one-quarter of the media transmitted in the first cohort, but this declined to 13% in the second and then to only 5% in the third. The incidence of sending photocopies (13% for the third cohort), actual parts or equipment (3% for the third cohort), and microfiche or shortwave radio transmissions (7% for the third cohort) remained roughly the same across the three time periods. Reliance on one's memory doubled from the first to the second cohort, and almost tripled in the third to 14%. Not

surprisingly, since 1990, the transmission of information by electronic files increased dramatically to 28%.

Meeting a recipient in person has been by far the most common method of transmission. More than three-fifths (63%) of methods chosen by those in the first cohort were meetings, and in the most recent cohort, meetings were the choice of 57%. In the second cohort, the predominance of meetings declined to 35%, and the proportion of instances with no attempt to transmit information—because the person had been prevented or intercepted before the attempt—increased to one-quarter of the total. Use of the telephone to transmit information increased over time, while the use of a courier, dead drops, and the mail or telegrams all declined.

Locations chosen for transmission, usually during meetings, have most commonly been outside the U.S., either because the spy was already located abroad or in order to evade monitoring and counterespionage activities undertaken by U.S. authorities. Half of the locations for transmittal in the first cohort were outside the country, while in the second and third cohorts, this decreased to roughly one-third.

A location out of town from where the spy lived or worked was the second most popular choice for transmitting information by the first cohort (12%), and remained the choice of 12% and 14% in the second and third cohorts, respectively. Post office boxes and parking lots have not been common choices in any cohort. Going to a foreign embassy has been the location for 15% of instances in the first cohort, 11% in the second, and 10% in the third. Hotel or motel rooms were no spy's choice of location in the first two cohorts, but since the FBI has honed its sting techniques to collect evidence by recording conversations in hotel rooms, these locations were used by at least 10 individuals in the recent cohort.

As in the previous variable on methods of transmission, there were more interceptions before transmittal was attempted in the second cohort (35%). There also has been a steady increase in other locations of transmittal, and this became one-quarter of the total for the most recent cohort, including transmission while in restaurants, grocery stores, cars, and by downloading over the Internet from classified networks while at places of work or by sending emails from home.[14]

[14] When the PERSEREC Espionage Database was first being developed, the possibilities of classified networks, downloading information over an Internet, or sending information or documents as attachments by email did not commonly exist. As these resources gradually became available during the 1990s and in the following decades, these new methods and locations used in espionage-related actions were coded as "other." This initial lack of interest in the details of emerging methods in itself illustrates that our coders did not at first recognize the importance of the shift to reliance on information technology, and the large impact it would have on espionage. The shift happened gradually.

## CONSEQUENCES OF ESPIONAGE

The consequences of getting caught spying vary from light punishments to life in prison. Table 8 reports on how espionage offenders were detected, and then on trends in payment, initial prison sentences, and outcomes other than prison.

**Table 8**
**Consequences of Espionage**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n = 66 methods* | % | *n = 85 methods* | % | *n = 107 methods* | % |
| Known methods of detection[15] | | | | | | |
| Surveillance | 21 | 32 | 24 | 28 | 38 | 36 |
| Tip | 22 | 33 | 25 | 30 | 24 | 22 |
| Confession | 4 | 6 | 11 | 13 | 9 | 9 |
| Offer for sale | 2 | 3 | 8 | 9 | 8 | 7 |
| Telephone tap | 2 | 3 | 7 | 8 | 10 | 9 |
| Other | 15 | 23 | 10 | 12 | 18 | 17 |
| | *n=54 persons* | % | *n=68 persons* | % | *n=50 persons* | % |
| Payment | | | | | | |
| None | 19 | 35 | 41 | 60 | 34 | 68 |
| $50 – $999 | 3 | 5 | 7 | 10 | 0 | 0 |
| $1,000 – $9,999 | 7 | 13 | 7 | 10 | 4 | 8 |
| $10,000 – $99,999 | 15 | 28 | 8 | 12 | 9 | 18 |
| $100,000 – $999,999 | 7 | 13 | 4 | 6 | 3 | 6 |
| $1 million or more | 3 | 5 | 1 | 1 | 0 | 0 |
| | *n=67 persons* | % | *n=72 persons* | % | *n=66 persons* | % |
| Initial prison sentence, in years | | | | | | |
| None | 15 | 22 | 6 | 8 | 3 | 4 |
| .1 – 4.9 years | 8 | 12 | 15 | 21 | 28 | 42 |
| 5 – 9.9 years | 10 | 15 | 14 | 20 | 13 | 20 |
| 10 – 19.9 years | 13 | 19 | 14 | 20 | 11 | 17 |
| 20 – 29.9 years | 4 | 6 | 10 | 14 | 2 | 3 |
| 30 – 39.9 years | 4 | 6 | 6 | 8 | 5 | 8 |
| 40 years | 2 | 3 | 1 | 1 | 0 | 0 |
| Life in prison | 11 | 17 | 6 | 8 | 4 | 6 |

[15] This variable shows the number of known methods of detection, not the number of individuals as in the subsequent variables in this table. All methods of detection mentioned for each individual are coded, and an individual may have used more than one method. For example, among the first cohort of 68 individuals, there were 21 instances of surveillance leading to detection. There were 22 tips, four confessions, two offers to sell information, two wire taps, and 15 other methods of detection, for a total of 66 methods. To get a percentage, each method is divided by the number of that type of method for the cohort (e.g., for surveillance in the first cohort: 21/66 = 32%).

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=14* | % | *n=5* | % | *n=2* | % |
| Outcomes other than being sentenced to prison at trial | | | | | | |
| Discharged | 2 | 14 | 0 | 0 | 2 | 100 |
| Defected | 5 | 36 | 3 | 60 | 0 | 0 |
| Granted immunity | 1 | 7 | 2 | 40 | 0 | 0 |
| Suicide | 4 | 29 | 0 | 0 | 0 | 0 |
| Died | 1 | 7 | 0 | 0 | 0 | 0 |
| Exchanged | 1 | 7 | 0 | 0 | 0 | 0 |

The unit of analysis in the first variable in Table 8 is the method of detection rather than the person. How a person was detected is a sensitive piece of information usually withheld from the public by counterintelligence and law enforcement authorities in order to protect sources and methods. As a result, what does appear in open sources is often vague, implied, or even doctored by those authorities.

Based on limited available data for each cohort, roughly three-fifths of the known detection methods involved surveillance or getting a tip. The other methods—confession to the crime, making an offer for sale, and use of a telephone tap—were less common. A variety of detection methods were coded as "other", including: discovery by various kinds of monitoring (e.g., video, Internet, and counterintelligence monitoring); physical search by police in the course of responding to another crime; captured documents from the Iraq War; suspicious polygraph results; financial analysis of a person under suspicion; discovery in the course of committing another crime or as part of the investigation of a crime by an accomplice; and a recipient of information who turns the person in to the authorities.

The proportion of spies who received no payment at all increased from 35% in the first cohort, to 60% in the second, and 68% in the third. Across all three cohorts, 49% of those who received no payment were intercepted before they could transmit information and receive payment (46 of 94 individuals).[16] Another one-fourth of persons who were not paid acted from an ideological commitment or from divided loyalties to another country or cause.

Among those who were paid, the amount of money has uniformly decreased, from the first cohort in which 22 individuals (44%) made between $10,000 and $999,999, to the most recent cohort in which only 12 persons (24%) made that much money. Prior to their arrests, three spies in the first cohort became millionaires from their crimes (Larry Wu-Tai Chin, John Walker, and Clyde Conrad), as did one person who began espionage in the 1980s (Aldrich Ames). No one from the most recent cohort received that much money.

[16] Interceptions are reported in Table 6.

## CONSEQUENCES OF ESPIONAGE

Espionage arrests usually end in prison. The number of individuals who received no prison sentence declined from 22% in the first cohort, to 8% in the second, and 4% of the third. The amount of prison time, however, has varied over the three cohorts. Twelve percent of people in the first cohort, 21% in the second, and 42% in the third received 1 to 5 years in prison. The next four categories—between 10 to 40 years in prison—generally declined over time as espionage drew somewhat lighter sentences. Eleven spies in the first cohort received life sentences, as did six in the second, and four in the third.

Outcomes other than a prison sentence were more common in the first cohort than in the others. Two individuals in the first cohort and two in the third were discharged, usually for prosecutorial misconduct or failure. Five persons in the first cohort and three in the second defected to the country to which they sent information before they could be prosecuted. One person in the first cohort and two in the second were granted immunity from prosecution. Four persons, all of whom were in the first cohort, committed suicide before they could be prosecuted. One person, Ruby Schuler, died from alcoholism during her investigation, and one person in the first cohort was exchanged for another prisoner.

## MOTIVATIONS

It is challenging to distill a person's motivations for espionage into a limited number of categories. Even when the categories appear to fit a crime as closely as possible, the nuances and idiosyncratic elements a person brings to motive are unique. Therefore, the analyses here try to capture two related dimensions of motivations. First, "strong motivations" correspond with a person's only or primary motive among several. Second, all known motivations over time are identified, including secondary and minor motives.

### Strong Motivations for Espionage

Table 9 lists individuals' strong motivations to commit espionage-related crimes across the three cohorts. This table differentiates between the number of persons who had a singular motive and the number of persons with multiple motives among which has been identified the primary motive. Where evidence suggested it, multiple motives were coded as primary, secondary, and tertiary. This was necessarily a subjective judgment because it was not based on personal interviews. When possible, it is most historically accurate to determine motivation from evidence available while the crime was being committed, rather than from the offender's self-justifications after the fact. Once caught, spies tend to justify their actions, and present their past intentions and the pressures that may have affected their behavior in an often generous light. For some individuals, however, their retrospective justifications are the only available evidence about their motives.

**Table 9**
**Strong Motivations for Espionage**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| Persons in each cohort | *n=68* | | *n=74* | | *n=67* | |
| Number persons with a sole motive | 44 | | 34 | | 22 | |
| Number persons with multiple motives | 24 | | 40 | | 45 | |
| | *n* | *%* | *n* | *%* | *n* | *%* |
| Money | | | | | | |
| Sole motive | 20 | 29 | 26 | 35 | 7 | 10 |
| Primary among multiple motives | 10 | 15 | 21 | 28 | 18 | 27 |
| | 30 | 44 | 47 | 63 | 25 | 37 |
| Divided loyalties | | | | | | |
| Sole motive | 8 | 12 | 3 | 4 | 9 | 13 |
| Primary among multiple motives | 7 | 10 | 10 | 14 | 15 | 22 |
| | 15 | 22 | 13 | 18 | 24 | 35 |
| Disgruntlement | | | | | | |
| Sole motive | 7 | 10 | 2 | 3 | 2 | 3 |
| Primary among multiple motives | 5 | 7 | 3 | 4 | 8 | 12 |
| | 12 | 17 | 5 | 7 | 10 | 15 |
| Ingratiation | | | | | | |
| Sole motive | 4 | 6 | 1 | 1 | 3 | 4 |
| Primary among multiple motives | 1 | 1 | 6 | 8 | 4 | 6 |
| | 5 | 7 | 7 | 9 | 7 | 10 |
| Coercion | | | | | | |
| Sole motive | 4 | 6 | 0 | 0 | 0 | 0 |
| Primary among multiple motives | 1 | 1 | 0 | 0 | 0 | 0 |
| | 5 | 7 | 0 | 0 | 0 | 0 |
| Thrills | | | | | | |
| Sole motive | 1 | 1 | 1 | 1 | 0 | 0 |
| Primary among multiple motives | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1 | 1 | 1 | 1 | 0 | 0 |
| Recognition or ego | | | | | | |
| Sole motive | 0 | 0 | 1 | 1 | 1 | 1 |
| Primary among multiple motives | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 1 | 1 | 1 | 1 |

Money consistently has been the strongest motive. In the first cohort, 44% of persons had a strong motive to spy for money, which increased to 63% during the 1980s. Commentators at the time expressed concern about a decline in American values when, during the Cold War, so many young people were willing to betray their country's secrets for money (Lentz, 1985). In the most recent cohort, however, money as a strong motive declined to 37%, which mirrors an increase in divided loyalties.

Divided loyalties is defined here as a commitment by American citizens to another country or cause they put before the U.S. This would include supporting or helping other nation-states, terrorist groups, or ideological systems, such as Communism. While spying from divided loyalties was a less important motive in the first two cohorts (22% and 18%, respectively), it grew in importance in the most recent cohort. In fact, divided loyalties rivaled money: among those who began espionage since 1990, 35% spied from divided loyalties (combining sole and primary motives), compared to 37% for money.

Why are there more divided loyalties among those who began espionage since 1990? The increase would seem to reflect at least three factors. First, people of the world have been knitted together by way of improved transportation and ICT, both of which help to foster and maintain foreign ties. Second, there has been an increase in the proportion of persons with ties to foreign nations who occupy jobs with access to sensitive or classified information. Third, the definition of espionage in this analysis has expanded to include leaks, economic espionage, foreign agent prosecutions, and export control cases alongside classic espionage.

Disgruntlement is the third most common motive, although it is often mixed in as a secondary or tertiary motive. It is defined as feelings of betrayal, disappointment, or resentment, usually caused by experiences in a job or professional setting. Only 11 individuals across the three cohorts committed espionage-related crimes solely from disgruntlement, but 16 others did so primarily from disgruntlement mixed with additional motives such as money or thrills.

Smaller numbers of individuals were motivated solely or primarily by ingratiation, coercion, thrills, or recognition. Ingratiation strongly motivated 10% or fewer people in each cohort. Coercion was a strong motive only in the first cohort with 7%. Thrills and recognition only served as strong motives for 1% of individuals in two of the three cohorts.

### Motivations through Time

Whereas Table 9 looked at strong motivations, Table 10 depicts motivation of any strength across cohorts. It answers the question: "How often was money a motivator in the first cohort?" and recognizes that inferring the relative importance of motives is subjective and inexact. Note that the unit of analysis in Table 10 is the motivation, not the person. The number of motivations by cohort is reported at the top of the table, and within that total is the number and percentage of each motive

for each of the three cohorts. Since some persons had multiple motives, those persons are counted more than once.

**Table 10**
**Motivations for Espionage through Time**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| Total motivations in each cohort | *n=100* | *%* | *n=129* | *%* | *n=134* | *%* |
| Money | 41 | 41 | 58 | 45 | 37 | 28 |
| Divided loyalties | 17 | 17 | 18 | 14 | 30 | 22 |
| Disgruntlement | 17 | 17 | 22 | 17 | 20 | 15 |
| Ingratiation | 6 | 6 | 12 | 9 | 22 | 16 |
| Coercion | 7 | 7 | 2 | 2 | 2 | 2 |
| Thrills | 10 | 10 | 10 | 8 | 5 | 4 |
| Recognition or ego | 2 | 2 | 7 | 5 | 18 | 13 |

The findings in Table 10 reinforce those reported in Table 9. Money remains the predominant motive, but in the recent cohort, it has declined to 28%, with divided loyalties a close second at 22%.

Figure 2 depicts these data for all motivations.

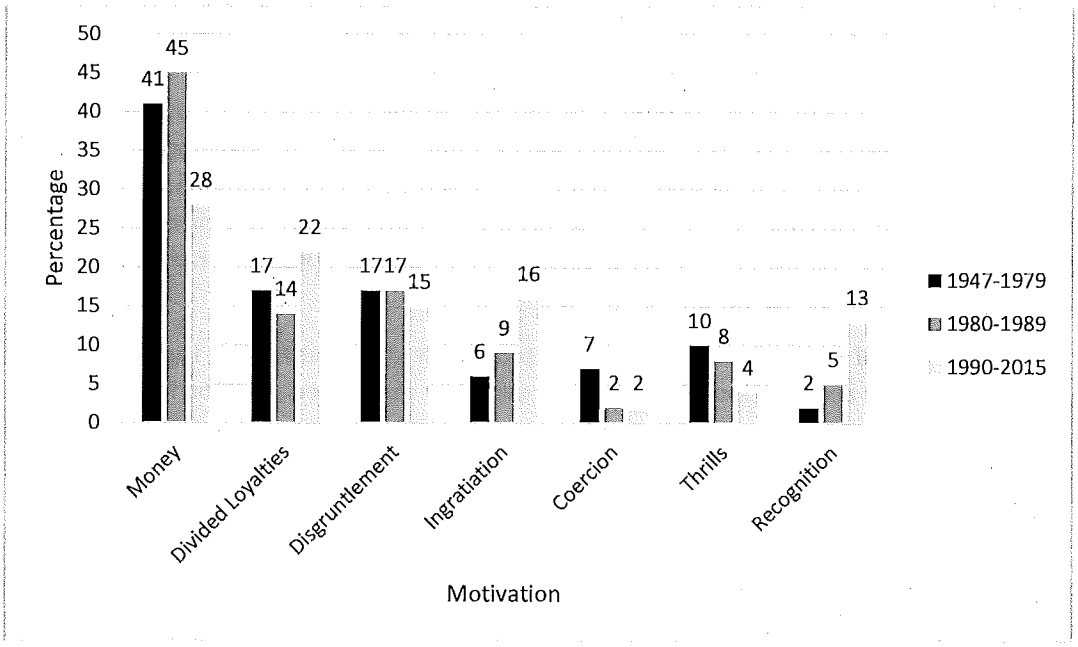



**Figure 2 All Motivations By Cohort**

### Examples of Spying for Money

The espionage case of Tai Shen Kuo and his accomplices provides an example of multiple motives. Kuo came to the U.S. in 1972 from his native Taiwan to attend college in Louisiana on a tennis scholarship. After he graduated, he stayed in New Orleans, became a naturalized citizen, and opened a tennis club, a restaurant, and then an import furniture store. Starting in the late 1980s, Kuo capitalized on his natural ability to make friends and develop useful contacts by expanding his business to China. Eventually, he established an office in Beijing, and became a matchmaker who could put American businessmen in touch with powerful Chinese officials (Arrillaga, 2011).

Kuo marketed American products and services to China for other friends. A mutual friend put him in touch with a contact in China, "a good person to know," who worked with one of the government-backed "friendship associations" that promote stronger ties with foreign nations while collecting intelligence by hosting visits to China. This contact worked for the Chinese government, and he became Kuo's backer and handler. He encouraged Kuo to find out from friends with government jobs about the U.S. government's attitudes toward the PRC and about its plans and intentions toward Taiwan (Klopott, 2009; Arrillaga, 2011; U.S. Attorney's Office Eastern District of Virginia, 2008).[17] Kuo gradually developed government sources who could provide him with such information, as well as with the answers to his contact's specific questions. One such source was his neighbor, James Fondren, Jr.

Kuo met Fondren in the late 1990s at their country club in Houma, Louisiana. Fondren had recently retired from the Air Force as a Lieutenant Colonel and was trying to start a consulting business. Kuo proposed that Fondren try writing opinion papers for his Chinese contact, whom he described as a friend in Hong Kong who worked in academia (Arrillaga, 2011). Fondren began writing papers based on his expertise on Asia, and Kuo would pay him between $800 and $1,500 per paper. Fondren wrote 30 papers between 1997 and 2008, which prosecutors later characterized as "thinly disguised regurgitations of classified military reports." Soon after he started producing these papers, Kuo invited Fondren to be his guest on a trip to China. They met Kuo's contact, played golf together, and enjoyed a scenic boat trip. Fondren's consulting business continued to boast only his first client, Tai-shen Kuo. For several years after that trip, Fondren and the Chinese contact exchanged dozens of emails on specific topics of interest to the PRC (Barakat, 2009).

---

[17] In 2009, the press was identifying Kuo's contact in China as Lin Hong, a Chinese intelligence officer (Klopott, 2009). In 2011, an article in the *Miami Herald* stated that Lin Hong had worked for the Guangdong Friendship Association in addition to being an intelligence officer (Arrillaga, 2011). While the affidavit filed in the Eastern District of Virginia for Kuo, Bergersen, and Kang identifies the contact only as "PRC official A", it places him as based both in Guangzhou and in Hong Kong (Affidavit, 2008). Guangzhou is the capital city of Guangdong province, also known as Canton, in the south of the PRC.

In 2001, Fondren returned to work for the federal government as deputy director of the Washington, DC, liaison office of U.S. Pacific Command. In that role, he regained his TS security clearance. He stopped corresponding directly with the contact, and worked only through Kuo. Kuo's contact demanded that Kuo send him more and better sensitive information. In response, Fondren wrote about topics that included official reactions to visits by Chinese military, joint Chinese-U.S. military exercises, intentions and plans for Taiwan, and insights into official American attitudes toward China. Some of these papers incorporated information classified Confidential or Secret. To assuage concern, Kuo told Fondren that his papers were being sent to government officials in Taiwan, but it is unlikely Fondren fell for that given his own relationship with the contact in China (United States District Court for the Eastern District of Virginia, Indictment, 2009; "Pentagon officials charged," 2009).

Kuo next developed Gregg Bergersen as a source. Bergersen was introduced to Kuo in 2006 at a party during one of Kuo's regular visits to northern Virginia. Bergersen, a Navy veteran, worked in the Pentagon as a weapons analyst for the Defense Security Cooperation Agency, which oversees foreign military equipment sales and tracks global weaponry. He and Kuo found each other mutually promising: Bergersen was thinking about retiring from the government and hoped his next step would be a lucrative consulting job, and Kuo told him he was setting up a defense consulting firm in Taiwan that would need partners like Bergersen. What Kuo actually wanted, however, was another government source with a TS security clearance and access to information on weapons policies and Taiwan. Bergersen believed Kuo's story that his information would be sent to Taiwan, and was thus taken in by Kuo's false flag operation (Montlake, 2008; Markon & Johnson, 2008).

Kuo cultivated Bergersen's friendship by taking him out to restaurants, on outings to various cities, and paying for trips to Las Vegas, where he underwrote Bergersen's gambling habit. Soon Kuo asked Bergersen to show him open source reports and plans from his office, and then asked for more restricted and even classified documents. In an infamous hidden camera video taken in a rental car, Bergersen and Kuo discuss a classified report for which Kuo puts a bundle of folded bills into Bergersen's shirt pocket. In the video, Bergersen is conflicted, claiming he will go to jail if anyone finds out he has shared the report. Kuo assures him he will only take notes from it. Kuo then takes the report into a restaurant and copies out large sections while Bergersen waits in the car.[18] Among other documents, Bergersen passed Secret information about Taiwan's upgrades to its C4ISR systems and also the U.S.' 5-year plan for military sales to Taiwan (Lewis, 2008; "Caught on Tape: Selling America's Secrets," CBS News, 2010).

[18] This video was included in a segment on *60 Minutes* on February 25, 2010, in which the video was shown interspersed with commentary by FBI and counterintelligence officers. The video was made public and is still available on the Internet, as is the *60 Minutes* segment.

Although he used email and phone calls to communicate with his Chinese contact, Kuo also sent his reports and documents to China using a cut-out, or a person used to create a gap between the supplier of information and the ultimate recipient. This cut-out, a young Chinese woman, was Yu Xin Kang, Kuo's employee at the furniture store and his lover. Kang was a Chinese national, an intelligence officer, and a legal permanent resident in the U.S. At Kuo's request, she came to New Orleans in 2007 to serve as a courier, and traveled back and forth between New Orleans and her apartment in Beijing where she would meet Kuo's contact and hand over materials (Morris, 2008).

The FBI learned of Kuo, Bergersen, and Kang in 2007 in the course of investigating another Chinese espionage operation, this one in southern California, focused on Chi Mak, who was an electrical engineer at a defense contracting company.[19] The FBI secretly searched Chi Mak's home and found his address books that included Tai-Shen Kuo and Kuo's Chinese contact. They began to surveil Kuo during 2007 and 2008, following him to his meetings with Bergersen, tapping his phone and email, and tailing Kang. During this time, they also bugged Kuo's rental cars to get the incriminating videos of his meetings (Markon, 2008).

The FBI arrested Kuo, Bergersen, and Kang on February 11, 2008. Ironically, Kuo's arrest took place at the home of James Fondren, Jr., whom Kuo had come to visit. This prompted the FBI to look into Fondren, who was arrested in turn in May 2009. Kuo pled guilty to conspiracy to deliver national defense information to a foreign government, and was sentenced to 188 months in prison (15 years and 7 months) and forfeited $40,000. In 2010, his sentence was reduced to 5 years based on his "complete cooperation" with Fondren's prosecution, his good behavior in prison, and the relative seriousness of the information he betrayed. Bergersen pled guilty to conspiracy to disclose national defense information, and was sentenced to 57 months in prison (4 years and 9 months) and 3 years supervised release. Kang pled guilty to aiding an unregistered agent of a foreign government (Kuo), and was sentenced to 18 months in prison and 3 years supervised release (Associated Press, 2010).

Fondren was indicted in May 2009, went to trial in September, and was convicted of unlawful communication of classified information to an agent of a foreign government and lying to the FBI. He was sentenced in February 2010 to 36 months (3 years) in prison and 3 years supervised release (U.S. Attorney's Office Eastern District of Virginia, "New Orleans Man Sentenced," 2008 [Kuo]; U.S. Department of Justice, 2008; "Former Defense Department Official Sentenced," 2008 [Bergersen]; U.S Department of Justice, "Jury Convicts Defense Department Official," 2009 [Fondren]; U.S Department of Justice, "New Orleans Woman Sentenced," 2008 [Kang]).

---

[19] The Chi Mak case has been widely written up, and it is discussed in detail in the previous PERSEREC espionage report.

## MOTIVATIONS

Kuo was motivated by money, followed by divided loyalties to China and the thrill of balancing the precarious and complicated parts in his life as both an American entrepreneur and a spy for China. Bergersen's primary motivate also was money, although he denied this at trial and blamed his alcohol and gambling addictions. He also was motivated by ingratiation with his generous friend Kuo, and perhaps equally important, the recognition and career boost he expected from Kuo's offer to make him a partner in the defense contracting start-up in Taiwan. Money also seems to have been Fondren's motivation, perhaps mixed with recognition. Kang's motivation was professional, and also a desire to ingratiate herself with Kuo, on whom she had an emotional dependence. As an intelligence agent for China, her loyalties were not divided.[20]

Money may be the most common motive for espionage, but it also can express some underlying or unacknowledged need, as was played out by most of the individuals in the Kuo case. Wanting money, for example, can express indirectly various psychological forces that affect the spy. While this study does not take a psychological approach and does not include access to conversations or clinical interviews with convicted spies, other studies do report on these insights, which may usefully expand on the basic motives discussed here.

Based on clinical interviews with three spies—Earl Pitts, Robert Hanssen, and Brian Regan—one psychiatrist finds that while money may be the superficial motive, the underlying motive is most often a fear of failure, which he ascribes particularly to men. He explains, "The only meaningful fact is whether the prospective insider spy feels like a failure to the point of it being intolerable for him." This author goes on to describe 10 stages in the evolution of a spy, from initial motive to espionage behavior (Charney, 2010).

Another student of espionage emphasizes, "Espionage is a crime with complex, multi-faceted motivational factors that do not lend themselves to easy explanations," and these factors reflect "intersecting psychosocial forces" (Thompson, 2014). His interviews with convicted spies suggest that the personal and cultural meanings of money may be as motivating as the typical categories of financial need, greed, or debt. For example, Aldrich Ames' ostensible motive was money to pay off his debts, but in interviews later he was more self-aware. He shared, "I did it for the money . . . not because of what it could buy but because of what it said about me. . . . It said Rick Ames was not a failure" (Thompson, quoting Earley, 1997). Thompson goes on to discuss other psychological dimensions of espionage, and notes that some spies act from a simple pressing need for money coupled with an inability to delay gratification or plan their future in such a way that addresses this need without crime. For some, espionage can solve such a problem almost immediately (Thompson, 2014).

---

[20] Since Yu Xin Kang is a Chinese national, she is not in the PERSEREC Espionage Database, and is discussed here only in her role as a co-conspirator.

A third study elaborates on the typical motives for espionage by exploring how they may be intertwined with psychological impulses. It applies Robert Cialdini's six principles of interaction to how case officers successfully recruit agents.[21] Cialdini's principles are described as "patterns of behavior that occur in the same order and sequence every time a given stimulus is introduced," so they apply to any human interaction (Burkett, 2013). For example, the principle of reciprocation is at work when a recruiter approaches a target and offers a small favor or service. Once the target has been helped, he/she feels obligated to reciprocate and help the recruiter, which may lead to a series of exchanges with escalating consequences. Cialdini argues that this cycle of helping is automatic and built into the structure of human interactions.[22] As such, the responses would operate beneath the target's conscious awareness (Burkett, 2013).

### Examples of Spying from Divided Loyalties

Table 10 shows that divided loyalties are the second most important motive in two of the three cohorts, the first and the third. In fact, instances of divided loyalties that have motivated espionage-related offenses almost have doubled between the second and the most recent cohort. Gwendolyn and Walter Kendall Myers, discussed earlier, were motivated by divided loyalties. Taking no money, they spied for Cuba for 3 decades because of an ideological commitment to the Cuban revolution and the Communist regime that sustained it (Clark, 2010). Another example of divided loyalties is the puzzling case of Ben-Ami Kadish and his arrest for espionage in 2008.

Kadish was born in 1923 in Connecticut and moved to British Palestine at the age of four. He fought for Israeli independence, and served in both the British and the American militaries in World War II (Newman, 2008). He returned to the U.S. and became a mechanical engineer. Starting in 1963, Kadish worked at the U.S. Army Armament Research, Development, and Engineering Center at the Picatinny Arsenal in Dover, New Jersey, where he held a Secret security clearance (Department of Justice, "Man arrested," 2008). In 1990, Kadish retired and moved with his wife to a New Jersey retirement community where he participated in veterans' activities and support groups, organized religious events, delivered Meals on Wheels, and joined in on sports and community activities with his retiree neighbors (Newman & Fahim, 2008). Eighteen years after he left his Army job, the FBI arrested Kadish at his home, charging him with espionage for Israel between 1979 and 1985 while he worked at the Picatinny Arsenal (Johnson, 2008).

Kadish pled guilty to one count of participating in a conspiracy to act as an unregistered agent for Israel. From 1979 through 1985, he worked with Yosef Yagur, then a science advisor at the Israeli consulate in New York. Yagur would

---

[21] Cialdini's six principles are reciprocation, authority, scarcity, commitment and consistency, liking, and social proof.

[22] This is not to claim that reciprocation would automatically lead to espionage, but only that it would automatically lead to some helping response.

telephone Kadish and ask for specific classified documents and reports. Kadish then would remove the requested documents from the classified library at the Arsenal and take them home. Yagur would come to Kadish's home the same night and photograph the documents in Kadish's basement (Cowan & Chan, 2008; Department of Justice, "Man arrested," 2008). Among the roughly 150 documents Kadish shared with Yagur were materials on nuclear weapons classified "Restricted Data", information on the modified F-15 fighter jet with the caveat NOFORN, and a Secret document regarding the U.S. Patriot missile air defense system (Department of Justice, "Man arrested," 2008).

While Yagur was working with Kadish in the mid-1980s, he also was one of several handlers working with Jonathan Pollard, whose work as an analyst at the Naval Intelligence Command gave him access to highly classified material. Using the same method Yagur used with Kadish, only on a much larger scale, Pollard carried boxes of classified documents home from his office for Yagur to photocopy (Neumeister, 2008).

This flow of information from both Pollard and Kadish ended abruptly in late November 1985, when Pollard and his wife, Anne, were arrested and charged with espionage and Yagur fled to Israel. The Pollards' attempt to evade capture by claiming asylum in the Israeli embassy, only to be turned away by the guards at the gate, is one of the iconic images of the "year of the spy" (Olive, 2006). Thereafter, Yagur lived in Israel, but maintained his relationship with Kadish, who visited Israel in 2004. After his arrest in 2008, Kadish telephoned Yagur, who told him to lie to the FBI and say he did not remember events from so long ago. Kadish did initially lie, and he was charged with lying to the FBI, but this charge was later dropped along with several others. Having pled guilty to the one count, in May 2009, a judge sentenced 85-year-old Kadish to a $50,000 fine. Kadish replied, "No problem" (Neumeister, 2009; Neumeister, 2008) and returned to his wife and his retired life.

What is puzzling about Kadish's arrest and prosecution is the timing and the reasons for pursuit after so long. The case set off considerable speculation in the press about whether there had been or continued to be sources working for Israel in the U.S., including a "super mole," long after the Pollards' arrest (Stein, 2008). People wondered whether Kadish's 2004 trip to Israel to see Yagur had set off the investigation, or whether the timing reflected political issues in 2008 between the U.S. and Israel. People also asked if the timing was meant to affect an upcoming leak trial of two lobbyists, Steven Rosen and Keith Weissman, who worked for the American Israel Public Affairs Committee (AIPAC) (Lewis and Johnston, 2009). Because Jonathan Pollard's supporters and the state of Israel itself have waged a vigorous effort to get his life sentence reduced and obtain his freedom, others speculated that prosecuting Kadish had something to do with preventing Pollard's

release from prison (Meiman, 2008; Neumeister, 2008).[23] These speculations, however, were not satisfied and the mysteries about Kadish's prosecution remain.

Table 11 depicts potential associations among a divided loyalties motive, citizenship status, and three variables on foreign preference.

[23] Jonathan Pollard was paroled on November 20, 2015, after serving 30 years. The terms of his parole include wearing an ankle bracelet and remaining in the United States for 5 years (Baker & Rudoren, 2015).

**Table 11**
**Divided Loyalties Motivation, Citizenship, and Foreign Preference[24]**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=68* | *%* | *n=74* | *%* | *n=67* | *%* |
| Citizenship | | | | | | |
| Born in U.S. | 53 | 79 | 62 | 84 | 44 | 66 |
| Naturalized | 15 | 21 | 12 | 16 | 23 | 34 |
| Persons with a divided loyalties motivation | | | | | | |
| Born in U.S. | 8 | 12 | 10 | 13 | 13 | 20 |
| Naturalized | 9 | 13 | 8 | 11 | 17 | 25 |
| | 17 | 25 | 18 | 24 | 30 | 45 |
| Persons without a divided loyalties motivation | 51 | 75 | 56 | 76 | 37 | 55 |
| Person had foreign relatives | | | | | | |
| Born in U.S. | 21 | 31 | 8 | 11 | 9 | 13 |
| Naturalized | 15 | 22 | 10 | 13 | 22 | 33 |
| No or unknown | 32 | 47 | 56 | 76 | 36 | 54 |
| Person had foreign connections[25] | | | | | | |
| Born in U.S. | 6 | 9 | 6 | 8 | 19 | 28 |
| Naturalized | 6 | 9 | 8 | 11 | 20 | 30 |
| No or unknown | 56 | 82 | 60 | 81 | 28 | 42 |
| Person had foreign cultural ties | | | | | | |
| Born in U.S. | 1 | 2 | 6 | 8 | 14 | 21 |
| Naturalized | 5 | 7 | 5 | 7 | 20 | 30 |
| No or unknown | 62 | 91 | 63 | 85 | 33 | 49 |

As discussed earlier, both the number of naturalized citizens and the number of divided loyalties as a motive almost doubled in the most recent cohort. Naturalized citizens, by definition, would have ties to their country of origin, so it is not surprising that most of them have foreign relatives, foreign connections, and/or foreign cultural ties. More revealing in Table 11, however, are the notable percentages of native born American citizens with these ties. These data suggest that while there has been an increase in the number of naturalized citizens in the

[24] Table 11 reports the number and percentage of persons with foreign relatives, connections, or cultural ties by citizenship status. A person may have more than one of these three ties, or may have none of them. Most persons in the PERSEREC Espionage Database did not have these ties, or it was unknown whether they had them.

[25] Foreign connections are defined as business or professional relationships, and/or acquaintances. Foreign cultural ties are defined as the person speaks the language of origin at home, maintains memberships in groups with a focus on the country of origin, or participates in political or educational activities in the country of origin.

recent cohort of spies, the increase in divided loyalties should not be attributed only to them.

### Ingratiation, Coercion, Thrills, and Recognition

The findings on ingratiation strengthen when Tables 9 and 10 are compared. Although not important as a strong motive in Table 9, ingratiation increases as a motive across the three time periods in Table 10. From 6% in the first cohort and 9% in the second, ingratiation accounted for 16% of motives in the recent cohort.

Coercion has declined in frequency over time, from seven persons in the first cohort to just two in the second and third cohorts, likely because the two most common blackmail risks have largely disappeared. First, the Berlin Wall fell after November 1989, and thereupon the Soviets abandoned the Iron Curtain that had kept people trapped in Eastern Europe from which their relatives in the West could be blackmailed. Secondly, the legal and social acceptance of homosexuality began to accelerate in the U.S. Threatening to harm a person's relatives living under Communist control in Eastern Europe, or threatening to publicly reveal one's sexual identity, have not been effective coercion strategies in the last two cohorts. It is possible, however, that new types of coercion will emerge given the emergent configuration of transnational terrorism.

Spying for the thrill of it has neither been a strong motive, nor has it increased over time, yet it has persisted as a secondary or tertiary motive. Some spies enjoyed an emotional rush from the danger they faced while spying, and some like Robert Hanssen thrived on beating the system (Vise, 2002).

The increase in recognition as a motive for espionage in the recent cohort is telling. Recognition refers here to a desire to be recognized and rewarded for one's accomplishments or talents, whether publicly or privately. Recognition includes elements of satisfying one's ego, since recognition involves gratifying the sense of self, but it is a more specific concept that better captures ambition for advancement in job or career, and/or a desire to exert influence and make a mark on the world.

### Helping and Ingratiation

Helping is a common theme in the explanations of espionage offenders' actions. "We weren't motivated by 'anti-Americanism,'" Walter Kendall Myers said at his sentencing hearing. "Our objective was to help the Cuban people defend their revolution" (Perez, 2010). "I thought I was helping the state of Israel without harming the United States," Ben-Ami Kadish said about his actions (Neumeister, 2009). "I believe our government's policy towards Cuba is cruel and unfair," Ana Montes explained at her sentencing in 2002. "I felt morally obligated to help the island defend itself from our efforts to impose our values and political system on it" (Golden, 2002).

**MOTIVATIONS**

Individuals who act on divided loyalties reject the exclusive commitment of allegiance, and often claim they are above allegiance to a single nation. By helping another country, they imagine they are on a higher moral plane. "I'm Chinese, I'm American," Dongfan Chung's wife[26] told a journalist after her husband's sentencing for economic espionage. "How beautiful is that! Why make it a confrontation?" (Bhattacharjee, 2014).

A desire to help, however, is not limited only to those whose divided loyalties led them to commit espionage-related offenses. As noted earlier, Table 10 shows that ingratiation has gradually increased with time, from 6% and 9% in the first two cohorts to 16% in the most recent. To ingratiate is to establish oneself in another person's good graces or favor, usually through deliberate effort.

The individuals who spied to ingratiate themselves usually claimed that they were trying to help the other person. For example, Rosario Ames, Virginia Baynes, and Marjorie Mascheroni were helping their husbands or lovers (Miller & Pincus, 1994; O'Harrow, Jr., 1992; Department of Justice, 2013). Frederick Hamilton, Michael Schwartz, and Lawrence Franklin were, they thought, sharing information with confidants to assist a close ally of the U.S. or even prevent a possible war (i.e., Hamilton in a confrontation between Ecuador and Peru, Schwartz by helping Saudi Arabia, and Franklin by heading off a war he thought was coming between Israel and Iran) (Gertz, 1993; "Norfolk Naval officer," 1995; Gertz, 2009). Nathaniel Nicholson was helping his imprisoned father (Denson, 2001). Donald Keyser was helping his lover with her graduate research—unfortunately she was a Chinese intelligence agent (Gerstein, 2006). Ryan Anderson and Hassan Abujihaad were trying to help Al Qaeda advance its agenda by sharing classified military intelligence (Kershaw, 2004; United States Department of Justice, 2009). Gary Maziarz was helping the Los Angeles County Terrorist Early Warning Center by sharing classified intelligence with uncleared task force members (Rogers, 2008) and John Kiriakou was helping journalists by acting as an expert source (Coll, 2013).

In addition to helping and ingratiating oneself, there often is a personal relationship at the core of an espionage case. When a spy offers or is recruited to supply information, the recruiter typically becomes the spy's first handler and serves as a link to the ultimate recipient. The role of handler is a demanding and delicate one that requires managing the spy's anxieties, responding to crises that may interrupt the smooth course of the espionage, and encouraging the spy to continue a perilous activity. Because the spy is in a vulnerable position, he/she becomes dependent on

[26] Ling Chung was not indicted for economic espionage, although she likely knew about her husband's espionage because papers were piled throughout her home. She also knew that her husband was sending materials to China and making presentations based on them in China.

the handler and may want to help in return for care and protection.[27] One CIA study of the psychological dimensions of espionage describes the relationship that can develop as follows:

> Adept professional handlers depict themselves not only as willing to reward espionage but also as capable of safeguarding their agent. Good professional "handling" is designed not only to collect classified information but also to stabilize and reassure the spy in the interest of sustaining his or her capacity to commit espionage for as long as possible. As a result, the relationship between an agent and a handler is frequently highly personal, intense, and emotional, at least from the perspective of the spy, and the nature of this relationship is often a powerful force behind an individual's choice to spy. ("The psychology of espionage," n.d.)

Robert Hanssen, for example, developed an emotional relationship with his various Russian handlers during the 15 years, off and on, that he passed highly classified documents from several government agencies. Cautious to the point of obsession, and insistent that everyone should follow the contact procedures he had specified to ensure his security, Hanssen would be upset when a mistake or an unexpected event caused a missed communication. In March 2000, less than a year before his arrest, he wrote to his handler and left the letter at a drop site in his neighborhood park:

> I have come about as close as I ever want to come to sacrificing myself to help you, and I get silence. I hate silence... Please, at least say goodbye. It's been a long time my dear friends, a long and lonely time. (United States District Court for the Eastern District of Virginia, United States of America v. Robert Philip Hanssen, Affidavit, 2001)

In November of that year, he explained his anxiety to his handler in more detail:

> (For me breaks in communication are most difficult and stressful.) Recent changes in U.S. law now attach the death penalty to my help to you as you know, so I do take some risk. . . . I had no regular way of communicating [with you]. This needs to be rectified if I am to be as effective as I can be. No one answered my signal [at the drop site]. Perhaps you occasionally give up on me. Giving up on me would be a mistake. I have proven inveterately loyal and willing to take grave risks which could even cause my death. (United States District Court for the Eastern District of Virginia, United States of America v. Robert Philip Hanssen, Affidavit, 2001)

---

[27] Two of Robert Cialdini's six principles seem to apply in this discussion of helping: reciprocation, the obligation to help that is elicited by receiving an initial favor, and liking, the principle that people like others who are similar to themselves. Recruiters, and later handlers, deliberately emphasize their similarities to the spy. They use flattery and they try to develop a personal relationship so the spy may come to feel "the case officer is one of the few people, perhaps the ONLY person, who truly understands him." (Burkett, 2013).

**MOTIVATIONS**

An overview of research on fraud, a crime that is often similar to espionage, notes, "We like to help each other, especially people we identify with. And when we are helping people, we really don't see what we are doing as unethical" (Joffe-Walt & Spiegel, 2012). In fraud, as in espionage, the long-term consequences tend to be distant and abstract, while the immediate benefits of the activities are much clearer. A spy contemplating the consequences of espionage knows on some level that these could be drastic, but also that they are in the future and may not even happen (Thompson, 2014). Ironically, then, helping, sacrifice, and altruism appear to wind their way through one of the most serious crimes a person may commit.

# PART 2

# TYPES OF ESPIONAGE BY AMERICANS

## FIVE TYPES OF ESPIONAGE

There used to be just one type of espionage. It was the type described in spy novels like those written by John le Carré or Graham Greene. It was the type reported in newspapers when someone with a security clearance like Aldrich Ames or John Walker stole a classified report or a cryptographic key card and handed it over for cash to an agent working for a foreign nation. It was the type everyone understood as what was meant by the term "espionage." It was classic espionage.

This report distinguishes among five types of espionage that have proliferated in the U.S. during the last several decades. One of them, the most frequent and best documented, is classic espionage. The other four types share basic elements with the classic type—and thus, are recognizably espionage—but they differ from classic espionage and from one another in obvious ways. The five types of espionage are:

- Classic espionage;
- Leaks of classified information;
- Acting as an agent of a foreign government;
- Violations of export control laws; and
- Economic espionage.

Economic espionage became a federal crime prosecuted as its own type of espionage under the 1996 Economic Espionage Act (EEA). Congress enacted this legislation to protect industrial and commercial information that forms the nation's economic base from theft by other nations in the same way the espionage statutes protect national defense information that forms the civic and military defense base. Specifically, the EEA criminalizes the misappropriation of trade secrets. One section applies to thefts done with knowledge or intent to benefit a foreign nation, and a second section applies to thefts done with knowledge or intent to injure the secret's owner.

The definition of a trade secret is based on the Uniform Trade Secrets Act (UTSA; as amended 1985), and specifies that such a secret can be many things:

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public. (Title 18 U.S.C. § 1831)

The other three types of espionage are not based on recent legislation, but instead are based on new, different, or more rigorous applications of older laws. Individuals who surreptitiously collect information in the U.S., or who advocate on behalf of and at the behest of a foreign power, have been legally required to register with the Attorney General since the 1938 Foreign Agents Registration Act (FARA; 18 U.S.C. § 1951). FARA exempts persons acting openly, because the concern is with clandestine activities on behalf of other nations. The information that is collected need not be classified. Some past classic espionage cases were prosecuted under both the espionage statutes and under FARA, but the number of persons in the recent past who were collecting information and sending it abroad, and who were prosecuted only under FARA, has increased.

The type of espionage defined by export control laws can be even more complicated than espionage involving an unregistered foreign agent. One of the main statutes that protects defense articles and technology is the 1976 International Traffic in Arms Regulation (ITAR), which authorizes publication of the U.S. Munitions List (USML). The USML includes 20 categories of controlled technologies that need not be classified, including specific weapons systems, aircraft and vessels, military electronics, nuclear weapons, space technology, satellites, and related technologies. Over the past 15 years, prosecutors have applied export control laws to various cases that involved selling systems on the USML to foreign powers.

The fifth type of espionage discussed here, leaks, also reflects changes in prosecution trends. Prior to the Obama Administration, there were only a few prosecutions involving controlled official information, almost always classified, that had been leaked to the press or to others not authorized to receive it. Under President Obama's Attorney General, however, at least a dozen leaks have been prosecuted, not always successfully.

These five types of espionage share elements intrinsic to an act of classic espionage, and are presented in Figure 3.

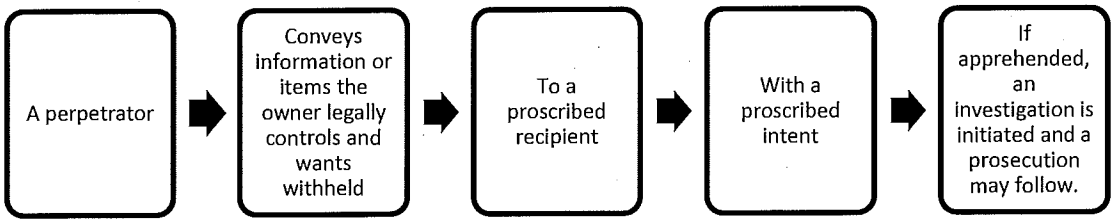



**Figure 3 A Model of Espionage Elements Based on Classic Espionage**

The elements in Figure 3 will be discussed for each of the five types of espionage considered in this report. In addition, notable cases for each of the five types will be explored, and for some examples, a standard checklist of elements derived from classic espionage cases will be applied to highlight similarities and differences.

Table 12 summarizes the types of espionage by cohort for the 209 Americans included in this report. Each offender's charges and conviction determined the type or types of espionage. Descriptions of what the person is reported actually to have done, even if evidence in court was lacking, also was considered. As Table 12 shows, prosecutors have charged individuals using both the espionage statutes and charges of a second type more often in the most recent cohort.

**Table 12**
**Types of Espionage by Americans**

| Characteristics | 1947-1979 | 1980-1989 | 1990-2015 |
|---|---|---|---|
| | *n=68* | *n=74* | *n=67* |
| | **Number of Persons Coded as One Type of Espionage** | | |
| Classic | 56 | 68 | 42 |
| Foreign Agent | 3 | 1 | 11 |
| Export Control | 0 | 1 | 4 |
| | **Number of Persons Coded as Two Types of Espionage** | | |
| Classic + Leak | 0 | 0 | 7 + Snowden[28] |
| Classic + Foreign Agent | 8 | 2 | 2 |
| Classic + Export Control | 0 | 0 | 1 |
| Economic + Foreign Agent | 1 | 0 | 0 |
| Export Control + Foreign Agent | 0 | 2 | 0 |

Table 13 presents only the counts and percentages of the classic cases, including those combined with other types of espionage, across the three cohorts, to highlight the predominance of classic espionage even more dramatically.

[28] Although he is discussed here, Edward Snowden is not included in the PERSEREC Espionage Database because he has not been tried or convicted of a crime. He is discussed only briefly in this report because he has talked openly about his actions, they are already widely reported and studied, and they have had an important impact on information security and the prosecution of leaks.

**Table 13**
**Percentages of Classic Espionage Cases**

| Characteristics | 1947-1979 | | 1980-1989 | | 1990-2015 | |
|---|---|---|---|---|---|---|
| | *n=68* | *%* | *n=74* | *%* | *n=67* | *%* |
| Classic | 56 | 82 | 68 | 92 | 42 | 63 |
| Classic + Foreign Agent | 8 | | 2 | | 2 | |
| Classic + Export Control | 0 | | 0 | | 1 | |
| Classic + Leak | 0 | | 0 | | 7 + Snowden | |
| Totals of Classic cases | 64 | 94 | 70 | 95 | 52 | 78 |

Almost all of the cases in the first two cohorts, 94% and 95%, involved classic espionage. If people were prosecuted for espionage, they were usually prosecuted under the Espionage Act, Title 18 U.S.C. § 792 through 798, which includes the core legal definition of classic espionage. Only in recent decades have different types of espionage been recognized, not always by that name, and defined by other statutes that have come into greater use or by existing statutes have been applied to in new ways. Thus, only 78% of cases in the most recent cohort involved classic espionage.

In January 2008, J. Patrick Rowan, the Deputy Assistant Attorney General in the National Security Division (NSD) of the Department of Justice (DOJ), testified before a U.S. House of Representatives subcommittee. He began his remarks on the enforcement of federal espionage laws in a way that neatly introduces the comparison of types of espionage that follows.

> It is my pleasure to appear before you today to discuss the National Security Division's enforcement of Federal espionage laws. As you know, the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but, increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons. Accordingly, these activities and others implicate a wide array of Federal criminal statutes. But no matter what form of espionage is being used, or which statutes are implicated, there is one common denominator: our national security is always at stake. (United States House of Representatives Committee on the Judiciary, 2008)

## ELEMENTS OF CLASSIC ESPIONAGE

Typically, classic espionage is defined as activities done for national government "A," which acts through an agent who clandestinely collects secrets from national government "B" that wants to control those secrets, and who turns them over to national government "A." Espionage is a subset of intelligence gathering; it is the illegal subset from the point of view of the government whose secret information is covertly being collected. Gathering information about potential adversaries involves some aspects that are legal and open, but usually these just support the clandestine activities.

The U.S., like many advanced nations, deploys a technologically sophisticated global intelligence gathering effort to ensure national security. As one part of that effort, U.S. agencies send identified and unidentified agents around the world to collect information that host nations would prefer remain under its control. These American agents, and their sources who provide information, are our spies (Sulick, 2013; Volkman, 1994). Unlike the spies America deploys, however, this report focuses on those Americans who work against their government. These are the original insider threats.

The context of classic espionage is a competition, a contest, or a struggle (CI Glossary, 2012; Manual for Courts-Martial, 2012).[29] At its most extreme, the context is international warfare. This means that espionage takes place in a context of "us vs. them," and an action that is reprehensible and illegal to those on one side will be judged as admirable or even heroic by those on the other. For example, the U.S. imprisoned CIA officer Aldrich Ames for espionage. In gratitude, however, for his valuable espionage, the Soviet Union funded a $2 million reward, which is being held for him in Russian banks (Earley, 2001).

The secrets in classic espionage are political or military in nature. Classic espionage has an ancient pedigree; examples can be found in the Bible, in ancient Greek and Chinese warfare, and throughout history in the wars and struggles between peoples up to the present. Consistently across that long history, the secrets sought through espionage involve military capabilities, new technologies, organizational structures, and foreign policies that address international intentions, goals, and relative strengths and weaknesses.

Since the end of World War II, governments have realized that economic health is as vital to a nation's future as its political and military secrets, and must be protected accordingly. It was a short step from that recognition to seeing the need to keep adversaries away from: technological advances; improved manufacturing methods; scientific breakthroughs; innovations in weaponry, space, and aviation; and the thousands of other developments that would be advantageous to other countries. From the triad of secrets in classic espionage—political, military, and economic—the need to protect additional kinds of secrets would grow.

---

[29] The summary of elements of classic espionage that follows is drawn from these sources.

Classic espionage usually involves theft. Stealing the secrets is an obvious and time-honored method for taking control of them and sending or transporting them to a recipient. Physically stealing secret documents or objects has recently been supplemented by electronically stealing secret files, plans, or communications. Other elements of classic espionage include surveillance and indirect theft. Observing, watching, and collating patterns of activities often can yield useful information, as can eavesdropping or performing computer sweeps where the adversary communicates unguardedly.

Subterfuge is commonly a part of classic espionage, which is to be expected given that it is both illegal and clandestine. The need to disguise and deceive plays out in many ways in the lives of espionage agents. They will create and enact cover stories and false identities to protect the true purpose of their activities. They may deceive their sources with false flag operations. Whether individuals volunteered to spy or were recruited by a foreign intelligence service, when they became spies they took up lives of double-dealing and its burdens. Because classic espionage is illegal and reviled by society as betrayal, the effort to maintain a false persona and to stay vigilant against possible discovery and arrest takes a psychological toll. What might at first seem like a romantic or thrilling adventure—to become a spy—seldom remains so as time passes.

Christopher Boyce, for example, spied for the Soviets for almost 2 years starting in 1975 at the age of 22. He stole highly classified documents from the Sensitive Compartmented Information Facility (SCIF) where he worked for the defense contractor TRW and handed them to his friend, Andrew Daulton Lee. Lee then traveled to embassies abroad and sold the documents to the Soviets. In August 1977, Boyce was convicted of espionage and sentenced to 40 years in prison.

In April 1985, Boyce was asked to testify before a Senate subcommittee investigating federal government security clearance programs (Lindsey, 1979; Serrano, 2003). Boyce detailed for the subcommittee the numerous security flaws and violations in his workplace, and his recommendations for improvements. He then told the Senators what it was like for him to be a spy for the KGB while he sat in his company's security briefings:

> [The briefer] stood there entertaining all those naïve, impressionable youngsters around me with tales of secret adventure, intrigue, huge payoffs, exotic weaponry, seduction, poisons, hair-raising risks, deadly gadgetry. It was a whole potpourri of James Bond lunacy, when, in fact, almost everything he said was totally foreign to what was actually happening to me.
>
> Where was the despair? Where were the sweaty palms and shaky hands? This man said nothing about having to wake up in the morning with the gut-gripping fear before steeling yourself once again for the ordeal of going back into that vault. . . . None of them knew, as I did, that there was no

> excitement; there was no thrill. There was only depression and a hopeless enslavement to an inhuman, uncaring foreign bureaucracy. I hadn't made myself count for something. I had made my freedom count for nothing. (United States Senate Committee on Governmental Affairs, 1985)

Yet, even after Boyce made his public statement in 1985, at least 97 additional Americans attempted espionage or espionage-related crimes against the U.S., including Glenn Duffie Shriver.

Shriver was interested in China. He spent parts of his college years at various study abroad programs in Shanghai, and after he graduated he returned to China, proficient in Mandarin, to look for work in 2004. In October, he answered an English-language advertisement looking for people to write "political papers." Shriver submitted a paper on relations among China, North Korea, and Taiwan to a woman named Amanda, who told him the paper was good. She asked if he would like to meet some other Chinese friends. Mr. Wu, Mr. Tang, Amanda, and Shriver met many times to get acquainted. The two men were curious about Shriver's career plans—had he considered applying for a job with the U.S. federal government, perhaps in law enforcement or diplomacy? Although he recognized a subtext of recruitment, one day Shriver asked them bluntly what they wanted, and he received an equally forthright answer: "If it's possible, we want you to get us some secrets or classified information" (United States District Court for the Eastern District of Virginia, "Statement of Facts", 2010; Wise, 2012).

Shriver agreed to try to get a job that would provide him with access to the kind of information the Chinese wanted. He applied to the Department of State (DoS) and took the Foreign Service examination, but failed it twice. Each time he took the test, the Chinese paid him for his trouble: $10,000 the first time, and $20,000 the second. In 2007, he applied online to work for the Central Intelligence Agency (CIA) in the clandestine unit—to become a CIA spy—for which he requested and received a $40,000 payment from the Chinese. He worked other jobs while he waited on the CIA's processing for several years, including supplying tattoo shops in Los Angeles and teaching English in South Korea. At some point during this period, he began to use the email codename "Du Fei," a play on his middle name. In late 2009, the CIA invited him to Washington, DC, for interviews and the supposedly final job processing, which took place in early May and June 2010 (Wise, 2012).

On June 21, 2010, as he boarded a plane to fly back to his job in South Korea, Shriver was arrested and charged with five counts of making false statements. In his CIA application, he had lied about not having had any contact with foreign representatives during the previous 7 years, about his travel to China in 2007, and about the $70,000 he had earned to date from Chinese officials (United States District Court for the Eastern District of Virginia, "Statement of Facts," 2010; Wise, 2012).

In October 2010, after interviews with the Federal Bureau of Investigation (FBI), Shriver was charged with one count of willfully conspiring with others, known and unknown, to obtain lawful possession of, access to, and control over documents and information relating to the national defense, which information the defendant would have reason to believe could be used to the injury of the U.S. and to the advantage of a foreign power, and thereafter to communicate, deliver, and transmit said documents and information to a person not entitled to receive it.[30] He pled guilty, agreed to cooperate in debriefings, and was sentenced to 48 months (4 years) in prison (United States District Court for the Eastern District of Virginia, "Plea Agreement," 2010). He never saw a classified document or gained access to any classified information, and although not acknowledged, it is likely that the CIA saw through his lies well before the interviews and the polygraph exam (Wise, 2012).

Shriver's case was an attempt at classic espionage. It also was an unusually bold effort by China's Ministry of State Security, the foreign intelligence agency, to groom and plant an American agent in the CIA. It illustrates many of the elements of classic espionage that were outlined earlier, including:

- A context of competition. The U.S. and the People's Republic of China (PRC) are in a vigorous, if not always open, international, economic, and geopolitical contest.
- Secret, clandestine actions. Shriver lied on federal application forms, smuggled cash payments back into the U.S. from China, and agreed to collect and transmit information to a foreign power in exchange for payment.
- Secrets. The Chinese intelligence service agents he met with were open with Shriver about their goal that he should collect secrets for them, and he was open with them about his attempts to get a job with classified access to obtain secrets.
- Political, military, or economic secrets. By encouraging Shriver to apply to DoS and to the CIA, the Chinese agents demonstrated that they wanted diplomatic or intelligence insights.
- Theft. Shriver was prevented from stealing secrets by being caught before he gained access.
- Subterfuge and surveillance. By being apprehended, Shriver also was prevented from exercising his tradecraft.
- Illegality. Shriver was convicted under two subsections of Title 18 U.S.C. § 793, one of the two most commonly applied espionage statutes.
- Psychological toll. Although he was not yet in a position to damage American interests, Shriver felt he had suffered from the attempt. At his sentencing he said, "By the time I came to realize I was in this situation, it was too late. . . . I cannot tell you what it's like to carry a dark secret like this for so many years" (Baracat, 2011).

[30] This reflects the language in Title 18 U.S.C. § 793(d) and 793(g).

About the same time that Glenn Shriver was taking and failing the Foreign Service examination in 2004 and 2005, a young U.S. Navy enlisted man was began his career as a spy. As Ariel Weinmann had approached his high school graduation in 2003, he had a steady girlfriend whom he wished to marry, but her parents opposed a son-in-law who intended to join the military. Leaving his girl behind but secretly engaged, he joined the Navy in 2003. He explained he was "looking for an adventure and I guess a degree of honor, something to make my life meaningful." He applied for a linguist rating but failed the tests, and became a submariner instead. He deployed as a Fire Control Technician 3rd Class on his first submarine in 2004 (McGlone, 2006).

Weinmann soon found that he disliked many aspects of life on the submarine, such as the fierce competition, the corruption and favoritism he observed, and the inefficiency. Slights and setbacks upset him, and they built into resentment against the Navy. For example, when the submarine returned to port, he drew orders to stand guard on the deck and thus, he missed his first homecoming port celebration, which he bitterly resented.

The first time he and his fiancée met when he returned home to Salem, Oregon, she handed back his engagement ring, broke off their relationship, and announced that her parents were sending her to college in Switzerland so she would be far away from him (Amos, 2006). On the spot, he began to think about how to desert the Navy and move to Austria, where he could use his fluent German, to be close to his girlfriend and try to win her back. Before he deserted, on July 1, 2005, he stole a laptop and downloaded classified files, including biographical compilations about 29 Austrians and technical manuals for the Tomahawk cruise missile system. He intended to barter this information for expedited asylum in Austria. He took his passport, his life savings, and a one-way ticket and boarded a plane for a series of flights that would take him to Vienna (Amos, 2006).

When Austrian officials at the airport refused to consider his request for expedited asylum, Weinmann settled into Vienna, drifting around waiting to hear from his girlfriend, who never called. He took up with a group of young Socialists who met in a park, including some Russians, and they became friends. Dropping the girl along with the notion of asylum in Austria, he decided to move to Russia. He then entered the Russian embassy in Vienna with a print-out of one of the manuals he had stolen. He handed the manual to the embassy officer, but then left with only a promise that the embassy would be in touch. Unfortunately, he failed to secure the *quid pro quo* he sought: Russian citizenship, a train ticket, and admission to a Russian university in exchange for his information. Realizing after he left that he had given away his only leverage, he next decided that instead of just moving there, he would defect to Russia and live there permanently. He prepared to leave Vienna by smashing the hard drive of the stolen laptop (McGlone, 2006).

On a series of flights on route to Russia, Weinmann first flew to Mexico City. Sources are ambiguous as to whether he may have tried to sell classified

information there. He also tried to arrange to be smuggled across the border into the U.S., but he did not have enough money for a guide. When he landed at the Dallas-Fort Worth Airport, a customs officer noticed his name on an active warrant for military deserters and he was arrested. After an international counterintelligence investigation that took months, he pled guilty to desertion, failure to obey a general order, espionage, copying classified information, larceny, and destruction of military property (Wiltrout, 2006b). Two additional counts of espionage were dropped. The military court sentenced Weinmann to 25 years in prison, reduction in rank to E-1, forfeiture of all pay and allowances, and a dishonorable discharge, but in a plea bargain, he would be serving only 12 years, and would be eligible for parole in 4 (White, 2006; Amos, 2006).

Weinmann stole classified information on a current weapons system and turned it over to a rival foreign power without being identified or stopped. Compared to the long-running and consequential espionage activities of John Walker, Robert Hanssen, or Aldrich Ames, Weinmann's case was probably minor, yet it demonstrates the elements of classic espionage:

- A context of competition. The U.S. and Russia have been major adversaries in a geopolitical and military contest that has waxed and waned for several decades.
- Secret, clandestine actions. Weinmann surreptitiously downloaded classified files from the Secure Internet Protocol Router Network (SIPRNet) while on the submarine. He planned to desert the Navy and use the information to his advantage.
- Secrets. The manuals for the Tomahawk missile system and the biographies that he downloaded were classified Secret.
- Political, military, or economic secrets. Weinmann downloaded the manuals because they could be attractive to an adversary. He meant the classified biographies of Austrians to be useful as a bargaining chip for expedited asylum in his original scheme to settle in Austria.
- Theft. Weinmann stole a laptop computer and downloaded stolen Secret files.
- Subterfuge and surveillance. Weinmann covertly stole the laptop, and he tried to be unobtrusive in his international movements by taking a series of flights on his way to his actual destinations. He flew to Chicago and then to Warsaw, Poland, before he landed in Vienna, and when he decided to defect to Russia, he first flew to Mexico City and then attempted to travel to Vancouver, Canada through Dallas.
- Illegality. Weinmann was charged and pled guilty to Articles 85 (desertion), 92 (failure to obey an order or regulation), 106a (espionage), and 134 (general activity that prejudices good order and discipline of the service) of the Uniform Code of Military Justice (UCMJ, U.S. Fleet Forces Command, 2006).
- Psychological toll. After his arrest, the Navy held Weinmann for 4 months during which time he was not in contact with anyone who could report publicly

on his state of mind (Wiltrout, 2006a). He is not reported to have made a statement at his sentencing, so his psychological status as he left for prison is undocumented.

### Classification and Legal Dimensions of Classic Espionage

Most classic espionage cases involve classified information. If it were compromised, classified information by definition would damage the U.S. to various degrees: the loss of Confidential information is defined as causing damage to national security; Secret information is defined as causing grave damage; and Top Secret (TS) information is defined as causing exceptionally grave damage (Executive Order 13526). Of the 209 individuals in this report, 186 persons (89%) committed classic espionage, either because what they did was in the classic pattern alone or because it is described as classic plus one other type.

Table 14 reports the clearance status at the start of espionage for the 186 individuals who committed classic espionage. Eighty-eight percent had access to classified information, including 134 with clearances, 10 who used their former clearances, and 20 who misused an accomplice's access to classified information.

**Table 14**
**Security Clearance Status at Start of Classic Espionage**

| Security Clearance | *n* | % |
|---|---|---|
| Total persons in this study | 209 | 100 |
| Persons coded as committing classic espionage | 186 | 89 |
| Of 186 persons who committed classic espionage, | | |
| Number holding security clearances at start of espionage | 134 | 72 |
| Number using their former security clearances at start | 10 | 5 |
| Number using the access of an accomplice | 20 | 11 |
| Total classic spies with access to classified information | 164 | 88 |
| Number who held no security clearance (e.g., stole information) | 13 | 7 |
| Number for whom security clearance status is unknown | 9 | 5 |

Access to classified information results from both a legal and moral agreement. Three elements are required in order to grant eligibility for a security clearance and to receive access to classified information. First, a person must demonstrate eligibility through a personnel security process that includes a background investigation and an adjudicative decision based on that investigation performed under the authority of a government agency head, who then becomes the sponsor

of that clearance. Second, the person must sign a nondisclosure agreement that legally binds the clearance holder in a contract to uphold the security requirements that apply to the information to which he/she has access. Finally, a person must have a need to know specific classified information, as determined by the local agency holding that information (Executive Order 13526).

The 144 individuals who held or previously held access to classified information broke the legal contract they signed in their nondisclosure agreements when they betrayed the trust invested in them. For persons who held clearances, many criminal complaints for espionage begin by referring to that very signature, which becomes one of the bases for prosecution.

Table 14 shows that 42 individuals involved in classic espionage cases did not hold security clearances. Several of those without clearances or former clearances stole information, while others attempted classic espionage with plans to secure future access. Some, however, passed information that was not classified.

Espionage prosecutions do not require information to be classified. The espionage laws date from the early 20th century and have evolved in a process more like accretion than revision, with new layers laid upon existing layers. The statutes date back to the 1911 Defense Secrets Act, which was the first law aimed at protecting the government's secrets. As the U.S. entered World War I, Congress enacted the Espionage Act in June 1917. This adopted the approach that had been taken in 1911 and incorporated many of its key phrases—which means that the espionage statutes are more than 100 years old (Elsea, 2013).

The series of provisions based on the Espionage Act are found in Title 18 U.S.C. section 792 through 798. Two of the sections most frequently used in espionage prosecutions are section 793, "Gathering, transmitting, or losing defense information," and section 794, "Gathering or delivering defense information to aid foreign governments."

Section 793 makes it a crime to disclose or attempt to disclose to "unauthorized persons" "national defense information" "with intent or reason to believe that the information is to be used to the injury of the U.S. or to the advantage of any foreign nation." It does not mention classified information, since classification of information did not exist in 1917 and was not introduced and standardized until World War II. It also criminalizes gathering or losing national defense information, terms that add to the broad yet vague problem with the statute. Penalties under section 793 include a fine and imprisonment of no more than 10 years (Elsea, 2006).[31]

[31] The following description of the statutes used to prosecute classic espionage is based on the excellent series of reports by legal scholar Jennifer Elsea for the Congressional Research Service (2006; 2013).

Section 794 proscribes passing national defense information to a foreign nation, or to any group within a foreign nation, "with intent or reason to believe that it is to be used to the injury of the U.S. or to the advantage of a foreign nation." Since it was written decades before transnational groups appeared, section 794 does not specifically provide for such a contingency as when the recipient of espionage is a non-state actor. It also treats conspirators who participate in the crime as equal to the actors who actually commit it. Section 794 is more serious than section 793 because it involves passing national defense information "to aid foreign governments," and so authorizes prison sentences of any length including life in prison or, if the crime resulted in the deaths of American covert agents or the compromise of major weapons systems including nuclear weapons, the death sentence (Elsea, 2006).[32]

As the early Cold War intensified during the late 1940s, and concerns about Soviet espionage grew, Congress passed the Internal Security Act (ISA) of 1950, which gave the espionage statutes the most thorough revision they have received to date. Three elements of the ISA are important in this discussion. First, this legislation added section 798, "Disclosure of Classified Information" to the espionage statutes inherited from 1917. Section 798 does specifically refer to information that has been classified, but the section applies only to information relating to codes, ciphers, and intelligence communications systems. Second, the ISA introduced a new section, 783, into Title 50 of the United States Code, "Communication of Classified Information by Government Officer or Employee", which defined it as a crime for "government officers or employees who, without proper authority, communicate classified information to a person whom the employee has reason to suspect is an agent or representative of a foreign government." This provided a second section that protects classified information by name, but again, its scope is limited in both the type of information protected and the category of persons to whom it applies (Elsea, 2013).

Third, the ISA separated one subsection of 793 that dated from 1917 into two subsections, and introduced new ambiguities in the process. The new subsections, (d) and (e), are, according to the most careful students of espionage law, "undoubtedly the most confusing and complex of all the federal espionage statutes" (Edgar & Schmidt, Jr., 1973). In trying to distinguish between persons with lawful possession (subsection d) and those with unauthorized possession (subsection e), the revisers introduced differences in wording that has required courts in subsequent cases to parse the subsections word by word, often reaching differing results (Barandes, 2007).

---

[32] Other sections in the Espionage Act criminalize specific and antique actions. For example, section 792 concerns harboring or concealing foreign agents, section 795 punishes photographing and sketching defense installations, section 796 calls out the use of aircraft in photographing defense installations, and section 797 punishes publication and sale of photographs of defense installations (Title 18 USC § 792-798).

These four laws, Title 18 U.S.C. § 793, 794, and 798 and Title 50 U.S.C. § 783, are the four most frequently used laws to prosecute classic espionage. There are, however, additional statutes that may also be applied depending on the circumstances of the crime and the nature of the evidence available. Other commonly used statutes include:

- 18 U.S.C. § 952 punishes employees of the U.S. who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, or coded materials in transmission between a foreign government and a U.S. diplomatic mission, with a fine and/or a prison sentence of up to 10 years.
- 18 U.S.C. § 1030(a)(1) punishes the willful retention, communication, or transmission of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information could be used to injure the U.S. or aid a foreign government. This provision also imposes a fine and/or imprisonment for not more than 10 years.
- 18 U.S.C. § 1924 prohibits the unauthorized removal of classified material. It applies to government officers or employees who "knowingly take material classified pursuant to government regulations with the intent of retaining the materials at an unauthorized location," and it imposes a fine of up to $1,000 and a prison term of up to 1 year.
- 18 U.S.C. § 641 punishes the theft or conversion of government property or records for one's own use or the use of another. It does not explicitly prohibit disclosure of classified information, yet it has been used in such cases. Violators may be fined and/or imprisoned for not more than 10 years.
- 42 U.S.C. § 2274 punishes the unauthorized communication by anyone of "Restricted Data", that is, data dealing with nuclear weapons or systems, or an attempt or conspiracy to communicate such data. If done with the intent of injuring the U.S., or in order to secure an advantage to a foreign nation, it calls for a fine of not more than $500,000 and/or a maximum sentence of life in prison. Other provisions punish with lesser sentences attempts or conspiracies to disclose such data.
- 50 U.S.C. § 421 protects information concerning the identity of covert intelligence agents. Intentional disclosure, learning the identity through exposure to classified information and revealing it, or learning the identity through a "pattern of activities intended to identify and expose covert agents" is subject to prison sentences of varying lengths from 3 to 10 years, and to fines. "To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the U.S. is taking affirmative measures to conceal. An agent is not punishable under this provision for revealing his or her own identity, and it is a defense to prosecution if the United States has already publicly disclosed the identity of the agent" (Elsea, 2006).

## ELEMENTS OF CLASSIC ESPIONAGE

Critics argue that the current espionage statutes are both too sweeping and general in scope, yet at the same time apply too specifically to technologies of the past so that they cannot cover the new permutations to espionage that have developed in recent decades. Therefore, they urge reforms (Vladeck, 2010). It is a real legal challenge to prosecute someone for espionage in the U.S. because of the inconsistencies and gaps in the available statutes (Bowman, 1995; Roth, 2001). Illustrating that challenge, the Counterespionage Section of the DoJ describes itself on its website as "providing legal advice on all matters within its area of responsibility, which includes 88 federal statutes affecting national security" (United States Department of Justice, Counterespionage/Counter Proliferation, 2015).

Of the 186 individuals described in Table 14 as committing classic espionage, 140 were charged, among other offenses, with one of the four main espionage statutes discussed earlier (i.e., Title 18 § 793, 794, and 798 and Title 50 § 783). Another 21 persons were charged under UCMJ article 106a (espionage) or article 106 (spies).

The remaining 25 individuals were charged under a related array of statutes including, but not limited to: Title 18 § 2071 (concealing, mutilating, or destroying government records); Title 18 § 1001(a) (making false statements to a government official); Title 18 § 1030 (willful retention, communication, or transmission of protected information obtained by accessing a government computer); Title 18 § 1924 (unauthorized removal of classified information by government employees, contractors, or consultants); Title 18 § 641 (theft or conversion of government property for one's own use or the use of another); Title 50 § 421(a) (disclosing information that identifies a covert agent); and the Atomic Energy Act, Title 42, § 2274 (communication of Restricted Data). They also were charged under various UCMJ articles, including: article 81 (conspiracy, in this case, conspiracy to communicate classified information to a foreign agent); article 92 (failure to obey lawful orders or regulations); article 85 (desertion); article 134 (general provisions, in this case, copying and attempting to deliver classified information to a person not authorized to receive it); and article 108 (selling government property) (Elsea, 2013; United States Department of Justice, Criminal Resource Manual, 2015; United States Department of Justice, Counterespionage/Counter Proliferation, 2015; Uniform Code of Military Justice, 2015).

Of course, being charged with various crimes is only a first step. The 209 individuals in this report, and specifically the 186 persons in classic espionage cases, were convicted of one or more espionage-related crimes, though not always under the core espionage statutes. Plea bargains, good defenses, and the lack of robust evidence to prove the most severe charges often have led to convictions and sentences that were reduced from the initial charges.

## LEAKS AS A TYPE OF ESPIONAGE

Leaks are disclosures of classified information to the public. They are usually accomplished through the press or by publication in print or electronic media. A leak follows the form of classic espionage except that the recipient is different. Instead of being given to an agent of a foreign power or transnational adversary, leaks go out to the American public. Then, through modern communication channels, the information is transmitted around the world as it is re-published, translated, and discussed in additional press coverage. Both the content of the information and the fact that it is no longer under the government's control are made available to everyone, including adversaries who systematically monitor the American press for insights.[33]

The general model of espionage elements that was introduced earlier in the discussion of classic espionage applies to leaks as well.

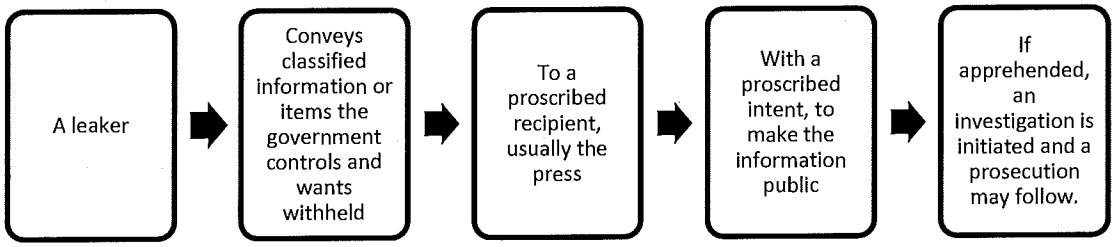



**Figure 4 Leaks in a Model of Espionage Elements**

A leaker's proscribed recipient is anyone who is: ineligible for a national security clearance, without authorized access, and/or without the need to know. Often, the leaker's proscribed intent is to make the information public in furtherance of a specific policy outcome or personal goal. There are, however, a number of motivations for recent leaks and it is instructive to compare them.

---

[33] Department of Defense, *DoD Information Security Program: Protection of Classified Information, Glossary,* Manual 5200.01-Volume 3, Enclosure 6, February 24, 2012a (as amended) defines an "unauthorized disclosure" as "communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient." Three levels of security incidents related to unauthorized disclosures are differentiated: 1) Infractions, defined as a failure to comply with requirements that does not result in loss or compromise; 2) Violations: security incidents that indicate knowing, willful, and negligent action that does or could result in loss or compromise; and 3) Compromise: security violation in which there is an unauthorized disclosure of classified information (where the recipient does not have a valid clearance, authorized access, or need to know). Loss is defined as a condition in which classified information cannot be physically located or accounted for (Summarized in Bruce & Jameson, 2013). The federal government considers classified information that has been made public to still be classified.

## LEAKS AS A TYPE OF ESPIONAGE

Leaks are a controversial phenomenon. Since Bradley Manning[34] and Edward Snowden released classified information, the impact and implications of those leaks and of all leaks has been widely debated.[35] Leaks are quite common, and trying to plug leaks also has been common. For example, between 2005 and 2009, 153 cases were referred to DoJ, which opened 26 cases and identified 14 suspects. Yet, not one led to an indictment (LaFraniere, 2013; Harris, 2010). During the Obama Administration, the Attorney General has prosecuted roughly a dozen individuals, thus prosecuting more leaks than in all previous decades since 1945 combined. This increase, and the aggressive use of mining electronic records that has enabled it, has been controversial (Lichtblau & Risen, 2009; Harris, 2010).

On the one hand, some argue these prosecutions can be unfair because the reality is that leaks represent a common currency in the relationship between reporters and government officials. They point to hundreds of leaks from the government each year, many of them intentional and authorized, and ask why only a few individuals are singled out for punishment while most go free. Some of these common leaks may be trial balloons that test out policies, or they are efforts to shape public perceptions before a competing policy becomes known, but others only serve the leaker's personal aggrandizement or reflect carelessness or callous disregard for security regulations (Caplan, 2013; Benkler, 2014).

The point of such arguments often is that, on balance, leaks can serve democratic governance, in their way, by preventing absolute government secrecy. Thus, the prosecutions and prison sentences for recent leaks seem to those who argue in this way to endanger the mechanism of leaking itself, which to them is a necessary check and balance on the government. In this view, leakers are akin to whistleblowers who show courage and initiative by revealing information they decide needs to be made public (Prepared statement of Gabriel Schoenfeld, 2010).

On the other hand, some support prosecution for leaks because classified information was designated as such for a reason, and releasing it without authorization endangers national security. People who argue for the strict prosecution of leaks emphasize the harm they have done and can do. To these commentators, leakers put their personal moral judgment above their legal responsibilities to comply with the rules on classified information to which they

---

[34] Manning announced he was changing his gender several days after he was sentenced in August 2013. Since he acted and was reacted to as a male during the time period of this summary, this description uses his original name (Bernstein & Tate, 2013).

[35] Many scholarly articles and book-length treatments prompted by the increased number of prosecutions of leaks have been published in the last 5 years. For a comprehensive article on legal, philosophical, and practical considerations of leaking classified information, see David E. Pozen, "The leaky leviathan: Why the government condemns and condones unlawful disclosures of information," *Harvard Law Review,* December 2013, 127(2), 513-635. Another useful and full discussion is by Gary Ross, "Who watches the watchmen? The conflict between national security and freedom of the press," Washington, DC: National Defense University, 2011.

themselves voluntarily agreed. These people are not whistleblowers, but more like miscreants or even traitors (Bruce, 2002; Wittes, 2014).

Concerns with over-classification (i.e., classifying information at a higher level than warranted and/or classifying too much information) buttress arguments from those who value leaks and advocate against criminalizing leaking. If what is claimed to be highly sensitive information that requires strict control turns out to be readily available open source information, agency gossip, or self-serving protection for poor agency decisions, then faith in the system is undermined and leaks look more justifiable. "When everything is classified," Justice Potter Stewart wrote in the Pentagon Papers decision in 1971, "then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion" (Quoted in Statement of Thomas Blanton, 2010). This is a thorny issue because if the leaked classified information was not actually sensitive, the leaker may try to argue it was improperly classified in the first place (Smith, 2010; Caplan, 2015).

An additional controversial element in the debate about leaks is the tension between the need for government secrets and the First Amendment. Not all leaks go to the press, but many do. Those who defend the press' right to publish leaked information argue for minimal restrictions and maximal trust in the reporters' judgment not to release information that is truly damaging. In contrast, those who wish to curtail leaks argue that reporters should be subject to legal sanctions when, ignoring classification markings, they knowingly publish information that, by definition, does damage, even if they do not realize it (Reporters Committee for Freedom of the Press, in Bruce, 2002).

These legal and political differences will not be completely resolved, but they could be rebalanced if calls for reform of the espionage statutes are heeded. Indeed, many commentators point to ambiguities in the laws as foundational to the argument about leaks.

The seven individuals prosecuted for leaks are presented in Table 15. Edward Snowden also is discussed, although he is not included in the PERSEREC Espionage Database because he has not been tried or convicted of a crime. Each of these cases illustrates distinctive aspects of the motives and circumstances that lead to a leak and each will be discussed in some depth.

**Table 15**
**Leaks**

| | Name/Age | Arrest Date | Employed by | Info Transmitted to | Type of Information |
|---|---|---|---|---|---|
| 1 | Lawrence Franklin<br>Age 52 | 2005 | DoD OSD, International Security Affairs, civilian | Steven Rosen and Keith Weissman, lobbyists for AIPAC | Classified information on Iran and Iraq |
| 2 | Matthew Diaz<br>Age 41 | 2006 | Navy, Judge Advocate General's Corps | Barbara Olshansky, attorney with the Center for Constitutional Rights, a NYC nonprofit for legal rights | Names of all the detainees at Guantanamo Bay, Cuba |
| 3 | Shamai Leibowitz<br>Age 39 | 2009 | FBI contractor | Richard Silverstein, an Internet blogger | FBI embassy transcripts on U.S. intelligence on Israel |
| 4 | Pfc. Bradley Manning<br>Age 22 | 2010 | Army | Julian Assange, WikiLeaks founder | DoS cables; Army reports and videos from Iraq and Afghanistan wars |
| 5 | Steven Kim<br>Age 42 | 2010 | DoS contractor | James Rosen, a Fox News reporter | Intelligence reports, analysis on North Korean nuclear plans |
| 6 | John Kiriakou<br>Age 42 | 2012 | Former CIA civilian | Scott Shane, a *NYT* reporter, and two other reporters | Identities of CIA intelligence officers; interrogation methods in use against terrorist suspects |
| 7 | Donald Sachtleben<br>Age 51 | 2013 | FBI contractor | An *Associated Press* reporter | Details on explosives used by the "underwear bomber" and FBI analysis of related bombings |
| 8 | Edward Snowden<br>Age 29 | 2013 | NSA contractor | Glenn Greenwald, a reporter for *The Guardian*, and Laura Poitras, a documentary filmmaker | Details of NSA domestic surveillance of communications, and U.K. and Israeli programs that were cooperating with NSA; ongoing revelations are continuing |

### Shamai Leibowitz

Shamai Leibowitz, a lawyer with dual American and Israeli citizenship, moved to Silver Spring, Maryland, in 2004. He worked for DoS teaching Israeli law and culture to diplomats for several years, and also for the Department of Defense (DoD) Defense Language Institute. From January to August 2009, he worked as a contract Hebrew linguist for the FBI, where he held a TS security clearance. He also blogged about political activism and moral and religious issues, and in April 2009, Leibowitz shared some 200 pages of classified transcripts from FBI wiretaps of

conversations that took place inside the Israeli embassy in Washington, DC, with another blogger and friend, Richard Silverstein. Silverstein, in turn, used some of the material from Leibowitz in his own blog. Based on the transcripts, Silverstein described telephone interactions among Israeli embassy officials and Jewish activists, members of Congress, and administration officials that could have embarrassed them.

While not a surprise that the FBI monitors Israel's communications, as it does other embassies, it is a sensitive practice that the FBI would prefer not be discussed in the press. The FBI began investigating soon after the leak in the summer of 2009, and on December 17, 2009, Leibowitz pled guilty to one count of violating Title 18 U.S.C. § 798, providing communications intelligence to a person not authorized to receive it. In May 2010, he was sentenced to 20 months in prison, but the court granted him 60 days to prepare to leave his dependent family (Kredo, 2010; Glod, 2010; Shane, 2011b).

Leibowitz admitted several motivations. First, he was uneasy with Israel's determined efforts to shape American public opinion and to lobby Congress. Second, he feared that, as reflected in the press of the time, Israel would attack Iran's nuclear facilities, thereby escalating an international crisis for the U.S. and Israel. As for Silverstein, when he realized the FBI was investigating Leibowitz in 2009, her burned the secret transcripts in his backyard and took down the reports from his website. He did, however, come forward publicly in 2011 to argue that Leibowitz had acted from a noble motive by trying to stop a rash attack on Iran. "I see him as an American patriot and a whistle blower, and I'd like his actions to be seen in that context," Silverstein told a reporter (Shane, 2011b). Leibowitz, on the other hand, wrote to the judge in May 2010,

> While working for the FBI, I came across information that troubled me very much and caused me to make a bad decision. I allowed my idealism and misguided patriotism to get ahead of me. . . . I made a mistake but only because I believed it was in the best interests of the American people. (Kredo, 2010)

### Stephen Jin-Woo Kim

Like Leibowitz, Stephen Jin-Woo Kim, a nuclear proliferation specialist, was working in 2009 as a federal contractor. Starting in 2008, he had been detailed to the DoS Bureau of Verification, Compliance, and Implementation from his job at the Lawrence Livermore National Laboratory. Kim was a respected senior intelligence analyst. He specialized in North Korea and had served as an adviser to various federal agencies on strategic nuclear deterrence. Born in Seoul, South Korea, Kim immigrated to the U.S. with his family at the age of eight, became a naturalized citizen, and earned degrees from Georgetown, Harvard, and Yale. Ironically, he tended to avoid the press and expressed concern about leaks to colleagues, but when a DoS public affairs officer asked Kim in March 2009 to talk

about North Korea with James Rosen, a reporter for Fox News, the two struck up an acquaintance (Apuzzo, 2010; Hsu, 2010; Marimow, 2013).

On June 11, 2009, the same day a CIA analysis on North Korea that required a Top Secret with SCI access (TS-SCI) clearance to view was released to only 95 specified analysts, including Kim, James Rosen reported online that "the Central Intelligence Agency has learned, through sources inside North Korea," that the North Koreans would respond to a United Nations Security Council resolution condemning North Korea for its nuclear and ballistic missile tests by launching another nuclear test, reprocessing their spent fuel, speeding up their uranium enrichment, and launching an intercontinental ballistic missile (Shane, 2011b; Pincus, 2013). The leak's reference to CIA sources and methods used to obtain intelligence inside North Korea incensed the CIA. Kim was investigated, questioned by the FBI, and indicted late in August 2010, when he was charged under Title 18 U.S.C. § 793(d), disclosing national defense information to a person not authorized to receive it, and Title 18 U.S.C. § 1001(a)(2), lying to federal officials (Apuzzo, 2010; Hsu, 2010; Marimow, 2013).

An affidavit supporting a request for a search warrant of May 28, 2010, demonstrates that DoJ investigators had pulled together electronic and communications records to startling effect. Rosen was working from a press office in the DoS building where Kim also worked, but in a secured section. The investigators correlated badging records with Kim's office desk telephone calls, office computer files, and emails to Rosen's cell phone and office desk phone. They also collected emails of all of Rosen's interactions with Kim, and conducted a late-night search of Kim's office. From these data, they reconstructed a detailed timeline of the relationship between Rosen and Kim between March and June 2009 (Marimow, 2013; United States District Court for the District of Columbia, Affidavit, 2010). They documented the dates, times, and durations of all calls between Kim and Rosen, including who initiated the call, dates and times for when each man left the building and when he returned, and incriminating emails illustrating how Rosen made Kim a source. For example, in a May 22, 2009 email, Rosen writes,

> "What I am interested in, as you might expect, is breaking news ahead of my competitors. I want to report authoritatively, and ahead of my competitors, on new initiatives or shifts in U.S. policy, events on the ground in [North Korea], *what intelligence is picking up,* etc. . . . I'd love to see some *internal State Department analyses* about the state of [North Korea]. . . . In short: Let's break some news, and expose some muddle-headed policy when we see it—or force the administration's hand to go in the right direction, if possible. The only way to do this is to EXPOSE the policy, *or what [North Korea] is up to,* and the only way to do that authoritatively is with *EVIDENCE."* (United States District Court for the District of Columbia, Affidavit, 2010) [Capitals are in the original and italics are in the original where they were meant to denote potentially classified information, now declassified.]

Both men knew their interaction was potentially sensitive. At Rosen's suggestion, Kim agreed to refer to Rosen in emails as "Alex" and to respond as "Leo Grace". They emailed one another using coded signals: one asterisk meant proceed with a communication plan and two meant hold off (Marimow, 2013; United States District Court for the District of Columbia, Affidavit, 2010).[36]

On March 29, 2010, in a second interview with the FBI, Kim tried to explain himself as agents laid out their timeline. He also tried to claim that he did not have an ongoing relationship with Rosen, and was not the source of the leak. In FBI notes of the interview, Kim is quoted as saying,

> I did not purposely discuss the [Intelligence Report], but might have discussed [some of the topics discussed in the Report]. . . . Maybe I inadvertently confirmed something . . . too stubborn to not . . . [I] just don't know . . . someone values my views, listens up . . . maybe I felt flattered. [The Reporter] is a very affable, very convincing, persistent person. [The Reporter] would tell me I was brilliant and it is possible I succumbed to flattery without knowing it. Maybe it was my vanity. [The Reporter] considers me an expert and would tell me . . . could use my insight. . . . The IC is a big macho game but I would never say I'm read in to this and you are not. I would never pass [the Reporter] classified. . . . [The Reporter] exploited my vanity. . . . My personal and professional training told me not to meet people like [the Reporter]. I felt like while on the phone I was only confirming what he already knew. I was exploited like a rag doll. [The Reporter] asked me a lot of questions and got me to talk to him and have phone conversations with him. [The reporter] asked me a lot, not just specific questions. [The Reporter] asked me how nuclear weapons worked. (United States District Court for the District of Columbia, Affidavit, 2010, Bracketed elements are in the original transcript of notes)

---

[36] DOJ investigators stepped around the law in order to gain access to Rosen's emails. A news report notes, "Privacy protections limit searching or seizing a reporter's work, but not when there is evidence that the journalist broke the law against unauthorized leaks. [In the Kim case], a federal judge signed off on the search warrant" after the FBI claimed that the evidence suggested that Rosen also had broken the law, "at the very least, either as an aider, abettor and/or co-conspirator" (Marimow, 2013). The DOJ later admitted they never intended to prosecute Rosen, but had claimed as much to portray him as a potential co-conspirator in order to get the search warrant and access to his emails with Kim. In July 2013, the Attorney General published new guidelines on leak investigations. "The new rules forbid the portraying of a reporter as a co-conspirator in a criminal leak as a way to get around the legal bar on search warrants for reporting materials" (Savage, 2013a; Savage, 2014). The possibility of prosecuting a reporter (Rosen) for receiving a leak of classified information (from Kim), which has never been done, caused an outcry from defenders of the freedom of the press, who argued that in order to gather information in the course of doing their jobs as national security reporters, they need to be able to discuss issues and receive information from officials in grey areas of classification and attribution. Lawyers for Kim argued that DoJ should drop the case or the judge should dismiss it, since Rosen's email records could not have been accessed under the new guidelines, but the DOJ refused and the judge refused to dismiss it on grounds the guidelines were only advisory and discretion remained (Marimow & Leonnig, 2013).

Early in February 2014, Kim pled guilty to leaking classified information to Rosen and to lying about it to the FBI. He signed a statement saying he was not a whistleblower. In early April, he was sentenced to 13 months in prison. At the sentencing hearing, defense counsel argued that Kim's interactions with Rosen were normal conversations between government officials and reporters, and "many of those conversations include the disclosure of classified information." The prosecutor countered that the "everyone-does-it argument" was not an excuse, and instead, Kim "was motivated not by an altruistic purpose but by his own ego and desire for professional advancement" (Marimow, 2014).

### John Kiriakou

From 1990 until 2004, John Kiriakou had an eventful career as a CIA case officer and counterterrorism specialist. In fact, he published a memoir of his experiences, which included recruiting agents in Athens while dodging assassination attempts, and assisting in the capture of Abu Zubaydah in Pakistan. After retiring, he went on to work for Deloitte in corporate intelligence, and also consulted on movies with intelligence or terrorism themes (Coll, 2013).

In December 2007, Kiriakou agreed to give a taped television interview with an ABC reporter about interrogation methods used on terrorism suspects, a controversy then gathering strength in the news. Although Kiriakou had not himself participated in interrogations, he confirmed based on what he had heard from CIA colleagues that waterboarding was being used, and that it had been used against Zubaydah. ABC claimed the interview made him the first CIA officer to confirm that the CIA had used waterboarding, a classified technique. In the interview, Kiriakou defended the CIA and the technique as having been fruitful for gaining valuable intelligence, but also admitted that he thought waterboarding was torture and probably should be discontinued (Coll, 2013; Shane, 2013a).

After his ABC interview, Kiriakou instantly became a favorite of news reporters looking for background on intelligence stories, confirmation of story lines, and names of others who could help develop stories. In several of his conversations with the press, he passed along classified information, including the names of covert agents who were still undercover (Coll, 2013; Shane, 2013a).

Kiriakou was prosecuted for leaking based on a conversation he had with a reporter who asked who at the CIA had led a program for the rendition of terrorism suspects to secret locations. At first he could not recall, but a few weeks later, Kiriakou sent the reporter an email in which he passed along the name he had just remembered. Later when asked, the reporter passed the name to an investigator who was working for defense lawyers representing Guantanamo Bay detainees. The investigator had been hired by defense attorneys to collect names and photos of CIA personnel who might have participated in interrogations of detainees, and who could become potential witnesses in their clients' future military trials. Specifically, the defense attorneys hoped to secure their clients' release by arguing that

detainees had been tortured during their interrogations and, therefore, any admissions were illegal.

In January 2009, defense lawyers submitted a classified motion to compel discovery of CIA documents which included the 81 names of CIA personnel the investigator had compiled (Coll; 2013). Some of those names were openly available, but others were not. Detainees themselves were found to have lists of names and accompanying photos of CIA personnel, which they received from their lawyers and passed around Guantanamo Bay to determine whether they could recognize their interrogators (Shane, 2013a; Federal Bureau of Investigation Eastern District of Virginia, 2012).

The CIA and the DoJ reacted to these lists with considerable concern because covert agents could be in danger from retaliation from Al Qaeda if their identities were revealed. The FBI worked to trace how these names and photos had ended up in the detainees' cells. The lawyers and their investigator explained their actions and methods, and convinced the FBI that they had been respectful, careful, and had kept within the scope of their role as legal counsel. The investigator pointed to the reporter as a source, and after the FBI got a search warrant for Kiriakou's email accounts, it became apparent that he had emailed the name to the reporter (Shane, 2013a; Coll, 2013).

The FBI investigated Kiriakou's various other media contacts, and in January 2012, charged him with three unauthorized disclosures of classified information, disclosing the name of a covert agent, and lying to the CIA and to federal officials. On October 23, 2012, Kiriakou pled guilty to one count of violating the Intelligence Identities Protection Act, and the other counts were dropped. He agreed to serve 30 months in prison. At his sentencing, the judge noted that she found the sentence "way too light" (Coll, 2013; Associated Press, 2012).

The flash points of American experience in the early 21st century run through Kiriakou's case, including the wars in Iraq and Afghanistan, the interrogation and detention of suspected terrorists at Guantanamo Bay and other sites, and the legality of interrogation techniques created in the years after 9/11. While Kiriakou seemed ambivalent about waterboarding in 2007, he eventually shifted his views and became a strong advocate against the use of torture. From his perspective, "After I blew the whistle on the CIA's waterboarding torture program in 2007," Kiriakou wrote to the *Los Angeles Times* from prison in 2014, "I was the subject of a years-long FBI investigation," which, he argued, considering all the highly placed officials who reveal classified information without penalty, had been unfair and discriminatory (Kiriakou, 2014).

### Donald Sachtleben

A fourth recent instance in which classified information was leaked to a reporter developed in May 2012. Its antecedents had begun several years earlier in 2009 with the thwarted Christmas Day bombing attempt of an airliner approaching

Detroit. The bomb came from Yemen and had been built into a passenger's underwear. In late April 2012, the CIA intervened in a similar plot in Yemen by Al Qaeda of the Arabian Peninsula (AQAP), which intended to bring down a plane using a new and improved underwear bomb designed without metal. Before the bomber could buy plane tickets, however, the CIA seized the bomb. The bomb then was flown to the FBI Laboratory in Quantico, Virginia, for forensic analysis, arriving on May 1 (Associated Press, 2012; United States District Court Southern District of Indiana, Indianapolis Division, 2013).

Donald Sachtleben retired from the FBI in 2008 after a 25-year career as a special agent bomb technician. He returned to the FBI as a contractor, and would periodically commute to the east coast from his home in Carmel, Indiana. On May 2, he entered the lab at Quantico, signed onto the computer system using his TS access, and walked across the hall into the room where the bomb was being examined. At 10:25 a.m., he called a friend, an Associated Press (AP) reporter, who had been texting Sachtleben to ask for any details on activities at the lab involving bombs from the Middle East. Sachtleben told his friend that there had been an interception of a plot in Yemen, and that a bomb had been recovered. He shared that the FBI was now busy with "an ongoing, secretive, and sensitive analysis of the bomb" with assistance from other U.S. government agencies, all of which was classified information (United States District Court Southern District of Indiana, Indianapolis Division, 2013).

After the government argued that sensitive issues in Yemen needed time to be resolved, the AP agreed to hold off publishing its story until May 7, the day before an official announcement about the incident was to be made. The FBI then began to investigate the leak. Over the next year, the FBI interviewed 550 people, but still did not have sufficient evidence to identify the leaker (Gerstein, 2013). DoJ then asked a federal judge to subpoena the telephone companies for records of 20 phone lines—including cell, office, and home—owned by AP reporters and the AP itself. Investigators compared the phone companies' records with other information, and identified conversations between the AP reporter and Donald Sachtleben, which led to search warrants for Sachtleben's computer files, cell phone records, and other electronic media (Savage, 2013c).

Investigators then discovered that the FBI already had custody of Sachtleben's computer. Nine days after he leaked the information from the FBI lab in Virginia on May 2, the FBI in Indiana arrested him for possession and distribution of child pornography and seized his electronics as evidence. The two cases swiftly merged, and Sachtleben pled guilty on September 23, 2013, to unauthorized disclosure of classified information, retaining classified information at his home, and one count each of possession and distribution of child pornography. In a plea bargain, he was sentenced to a combined 140 months (11 years 8 months) in prison, which included 43 months for the leak (Horwitz, 2013; United States District Court Southern District of Indiana, Indianapolis Division, 2013).

In addition to the immediate effect of revealing an ongoing terrorist investigation in Yemen, the Sachtleben leak had several other serious consequences. The subpoena for the 20 AP phone lines exacerbated public criticism associated with the Kim case in which the FBI had seized Rosen's email records using a search warrant. Criticism of these two leak episodes from vocal supporters of the freedom of the press successfully put pressure on the Attorney General, who issued new guidelines in July 2013 that made such records more difficult for prosecutors to obtain (Savage, 2013a; Gerstein, 2013). Also, further investigation by the press into the disrupted AQAP plot in Yemen suggested that, in reality, a Western mole had been designated to carry the bomb, but because the leak had prematurely revealed the plan, the mole was hurriedly extracted and the U.S. lost a valuable informant (Barrett, 2013; Gerstein, 2013).

### Bradley Manning

U.S. Army Private First Class Bradley Manning, age 22, deployed to the Iraq War with the 10th Mountain Division 2nd Brigade late in October 2009, and was stationed at Contingency Operating Station Hammer,[37] a combat zone east of Baghdad. He had trained as an intelligence specialist and was granted a TS-SCI security clearance. Manning spent 14-hour shifts in a SCIF, sifting through local intelligence reports and working with computer databases to improve the security of local military operations (Barnes & Hodges, 2010; Nakashima, 2011).

Between November 2009 and February 2010, Manning demonstrated increasingly erratic and disturbing behavior. During this time, he also explored online how he could contact WikiLeaks, an Internet site run by Julian Assange, which billed itself as a secure, anonymous place to download secrets and see them published without fear of being traced. Assange cultivated Manning and shared technical knowledge with him. In mid-February 2010, Manning began downloading large data files and whole archives of data onto writable CDs he brought into the SCIF disguised as music. He installed forbidden software on his work computers to assist with data search and identification, and he explored available content (Dishneau & Jelinek, 2011). In total, he stole over 700,000 documents and files, including some 150,000 DoS diplomatic cables sent from embassies around the world, Army field logs from the Afghanistan War, an embarrassing video of a U.S. Army helicopter apparently shooting at civilians on the ground, and hundreds of thousands of documents related to the Iraq War. The scale of the theft dwarfed all previous leaks (Nakashima, 2011; Shanker, 2010; Pilkington, 2013).

Manning's transfers to WikiLeaks continued in bursts during March, April, and May 2010, as did his outbursts of emotion and barely contained violence. WikiLeaks did not publish all of Manning's material, but it did publish the helicopter video on April 5, 2010, to instant notoriety.

---

[37] This also is referred to as Forward Operating Base Hammer in press accounts.

Manning was arrested on May 26 and held in pre-trial confinement during the 7-month leak investigation. After a psychological evaluation and a well-publicized trial, Manning was convicted on July 30, 2013, of 17 of the 22 charges in their entirety, and of amended versions of four additional charges. These included six of the eight counts brought under the espionage statutes (Title 18 U.S.C. § 793) for unauthorized disclosure of the Afghan and Iraq War logs, embassy cables, and files from Guantanamo Bay "with reason to believe such information could be used to the injury of the US or the advantage of any foreign nation." He also was convicted of "wrongfully and wantonly" causing the electronic publication of intelligence belonging to the U.S., "having knowledge that intelligence published on the internet is accessible to the enemy." He was reduced in rank to E1, the lowest possible rank, forfeited all pay, and dishonorably discharged. He was acquitted of the most serious charge, however, that of aiding the enemy by causing classified information to be published where the enemy would see it (Pilkington, 2013; Savage & Huetteman, 2013). On August 21, 2013, he was sentenced to 35 years in prison (Tate, 2013; Nakashima, 2011).[38]

Manning became "the first mass digital leaker in history," according to one account (Pilkington, 2013), and the incident was a shock due to its scale and the impunity with which WikiLeaks published the information.[39] Manning's behavior challenged untested assumptions about trust, and demonstrated how persons with broad access to automated systems and electronic files inside an organization could do serious damage (Shanker, 2010). In response, the White House issued Executive Order 13587, which required every agency to develop an insider threat program to audit, monitor, and evaluate the use of government computer systems by cleared personnel (Walker, 2013; Executive Order 13587, 2011; Department of Defense Directive, 2014; The White House, Near-term measures, 2014).

Manning's behavior has been the subject of hundreds of articles, character studies, government reports, legal treatments, and books. Here only two aspects, seen in hindsight, are discussed. They were chosen because they suggest how and why Manning was able to accomplish the leak, and they offer clues for mitigating future vulnerabilities.

First, the information security practiced at Contingency Operating Station Hammer in Iraq was inadequate, at best. Admittedly, a combat environment makes special demands on typical security procedures, but the base received classified and

---

[38] On January 17, 2017, President Obama commuted all but 4 remaining months of Manning's sentence and he was freed on May 17, 2017 (Savage, 2017).

[39] WikiLeaks did at first attempt to screen the classified information by working with three international newspapers: *The New York Times*, *The Guardian* in Britain, and *Der Spiegel* in Germany. These newspapers reviewed the documents Assange provided in order to develop their own stories, and while doing so their staff readers tried to filter out information that could endanger persons or betray particularly sensitive operations (Nakashima, 2010). This process of decrypting, screening, and publishing in batches went on for some months until a password was leaked, and Assange quickly released most of the remaining materials all at once without review (Nakashima, 2010; Bumiller, 2010).

sensitive information over SIPRNet that should have been carefully protected. Under lax supervision, Manning was able to install proscribed software, access additional data without authorization, bring removable devices disguised as music into the SCIF, download archives of data, and then encrypt and upload the files to the Internet and WikiLeaks (Nakashima, 2011; Jaffe & Nakashima, 2011).

Second, Manning's experience in the Army calls into question the approaches that were then in place to respond to troubled military personnel. Manning did not fit well in the military. He was short, slight, not athletic, moody, but very smart. Also, he struggled with his sexual and gender identity. Although this was during the time of "Don't Ask Don't Tell", Manning became more open with his sexuality with friends and also on Facebook. During his military career, he fell in love with a man for the first time and then suffered a break-up.

Manning complained repeatedly that he had no one to talk to about his troubles. He suffered from mood swings, depression, outbursts of aggression when frustrated, and made threats of violence toward others and himself. Despite numerous short-term interventions, officers overlooked the larger pattern that suggested a seriously troubled individual and sent Manning to Iraq because they desperately needed capable intelligence analysts (Youssef, 2011; Nakashima & Tate, 2011; Savage, 2013b; United States v. Manning, Defense request, 2011).

Once he arrived in Iraq, Manning's disillusionment with the American war effort became acute. For example, he was upset over his Army supervisor's lack of response to corruption in the local Iraqi police (Fishman, 2011). He knit all of his grievances into a plan of action. First, he would show the world the 2007 video of an American helicopter shooting at and killing two Reuters journalists and 12 Iraqi civilians. Then, so the world would know what was really going on, he would leak the logs of military operations in the Iraq and Afghanistan wars along with thousands of diplomatic cables that revealed America's foreign policy in candid detail. His disclosures would have implications of "global scope, and breath-taking depth," he told a hacker confidant, who later turned him over to the authorities (Nicks, 2010).

### Matthew Diaz

In 1995, Matthew Diaz joined the U.S. Navy's Judge Advocate General's (JAG) Corps as a staff attorney. In June 2004, the Navy sent him to Guantanamo Bay for a 6-month tour as the Deputy Staff Judge Advocate. A week before he arrived in Cuba to oversee the coordination of all detainees' potential legal contacts, the Supreme Court ruled in *Rasul v. Bush* that detainees held at Guantanamo Bay had a right to challenge their detentions in U.S. federal court (Wiltrout, 2006; Wiltrout, 2007; United States Department of the Navy General Court-Martial, Defense response, 2007). Later in 2004, lawyers offering to defend detainees based on *Rasul* tried to learn their names and countries of origin, but they found the Navy, the Pentagon, and the Bush Administration unwilling to divulge the information. A DoD

lawyer testified at Diaz's court martial that the Pentagon had no intention of making this information public by turning it over to potential defense lawyers who were requesting it based on a policy, "We do not publish lists of people captured in armed conflict" (Rosenberg, 2007a).

Early in January 2005, as Diaz's tour in Cuba was about to end, he saw himself in a "moral dilemma" (Scutro, 2007). He felt that what he characterized as the government's "stonewalling" was both morally wrong and illegal given the recent Supreme Court decision. Given his own father's incarceration, Diaz felt very strongly about this issue.[40] Knowing he would lose access at the end of his tour, Diaz printed out information about 551 detainees from a SIPRNet file, including names, countries of origin, and various codes that reflected what, if any, intelligence had been gleaned, and which interrogation team had been assigned to the individual (Scutro, 2007). He reduced the pages to index card size, cut the printout into 39 pages, and wrapped the pages in a valentine hoping to disguise the package as it passed through the base post office. On his last day in Cuba, he sent the package anonymously to Barbara Olshansky, a lawyer for the Center for Constitutional Rights in New York City (Golden, 2007).

The Center for Constitutional Rights is a nonprofit legal rights organization, and Olshansky was one of the lawyers in the *Rasul* case who was then suing for access to the detainees' names in federal court. Although the pages Diaz sent were not marked Secret, Olshansky correctly inferred when she opened the package that she did not have a legal right to view the contents. Mystified about why they had come to her and who had sent them, she turned them over to the federal court in which her suit had been filed. The judge, in turn, notified the FBI that potentially classified information had been disclosed. The FBI then used computer forensics, fingerprinting, and a national security letter that requested Diaz's emails to determine who had sent the classified information (Wiltrout, 2007; Rosenberg, 2007b; "Navy lawyer," 2007).

Charges against Diaz were made public late in August 2006. During the subsequent investigation, he continued to work as a Navy lawyer in Jacksonville, Florida. Eventually, Diaz was charged under the UCMJ with violating the Navy's information security program by mailing a classified document through the first class mail, and with conduct unbecoming an officer by transmitting a classified document to someone not authorized to receive it. He also was charged with three counts of violating the Espionage Act: making a printout of a classified document relating to the national defense with intent or reason to believe it would be used to injure the U.S. or for the advantage of a foreign nation; knowingly and willfully communicating that information to someone not authorized to receive it; and removing the information without authority with intent to store it in an

[40] Diaz's father was convicted of murdering 12 patients in his nursing care by injecting them with Lidocaine, and was sentenced to death in 1984. Despite his claim of innocence, he remained on California's death row until he died of natural causes in August 2010 (Cruz, 2010).

unauthorized location (United States Department of the Navy General Court-Martial, Defense response, 2007).

The court martial began in May 2007 in Norfolk, Virginia. According to his defense lawyers, "LCDR Diaz's billet placed him directly in the middle of the legal and logistical fallout from the Supreme Court's decision in *Rasul*" (United States Department of the Navy General Court-Martial, Defense response, 2007). In addition, the defense argued that the printout was not really classified—it was not marked as such, and all of the information on it already been made public in April 2006 in response to a Freedom of Information Act suit (Wiltrout, 2006). The prosecution, in contrast, argued that the printout had been classified when Diaz mailed it—it had come from SIPRNet and the Judge Advocate's office was a classified environment, of which Diaz was well aware (Scutro, 2007; Rosenberg, 2007a). Others testified that the information in the codes on the printout included intelligence sources and methods, and also the names of countries that did not want to be publicly identified (Rosenberg, 2007b).

Diaz was found guilty of four of the charges, which could have meant 14 years in prison. He was sentenced on May 18, 2007, to 6 months in prison and a discharge from the Navy, with the likelihood that his military pension would be forfeited due to the espionage-related conviction. "We think this will send a clear message that you can't just release classified information, no matter how good an intention you think you have," the prosecution commented during the trial (Wiltrout, 2007). Diaz spoke at his sentencing and defended his belief that the detainees were being treated unfairly and illegally, but he admitted that as a naval officer, his response was wrong. He admitted that other avenues had been available to him to register his disapproval of his government's policies, and he expressed shame that by sending the printout anonymously, he had not acted with the courage of his convictions. (Wiltrout, 2007)

### Lawrence Franklin

Lawrence Franklin was a South Asia specialist who worked the Iran desk in the International Security Affairs Office of the Office of the Secretary of Defense (OSD). He had earned a Ph.D. in Asian Studies, held a TS-SCI security clearance for 3 decades, and, in addition to his academic and policy roles in the federal government, served as a Colonel in the Air Force Reserve.

During the 1990s, Franklin developed a strong disagreement with American foreign policy toward Iran. He complained that the National Security Council (NSC) was not taking the Iranian threat seriously, and he fought an interagency battle among DoD, DoS, and CIA over evolving policies toward Iraq (Gertz, 2009). Starting in April 1999 and continuing until August 2004, Franklin tried to influence foreign policy by sharing classified information with various Israeli contacts, including Israeli embassy officials who were friends of his, and two American Israel Public Affairs Committee (AIPAC) lobbyists, Steven Rosen and Keith Weissman.

The information he passed along verbally to these individuals in meetings held in the Pentagon Athletic Club and in Washington, DC, coffee shops and restaurants usually consisted of insights into secret internal deliberations among U.S. policymakers, but it also included intelligence on military plans and potential attacks on American forces in Iraq ("Pentagon man," 2006; United States District Court for the Eastern District of Virginia, Criminal complaint, 2005; United States District Court for the Eastern District of Virginia, Superseding indictment, 2005). Franklin worried that as an attack on Iraq approached, the foreign policy community was not properly considering the preparations by and the likely reactions of Iran (Gertz, 2009).

Israel, a close American ally, denied conducting espionage against the U.S. through its embassy officials and American lobbyists, but starting in June 2003, FBI agents began monitoring Franklin's movements and communications, and collecting evidence against the three men. In June 2004, the FBI confronted Franklin and threatened him with a long prison term unless he wore a wire in a series of sting operations against the other suspects. Given that his wife was then confined to a wheelchair with multiple sclerosis and they had five children, Franklin agreed to cooperate against Rosen, Weissman, and others to whom they had passed the information. This included the political advisor to Ahmed Chalabi, a prominent exiled Iraqi politician who was then angling to become prime minister of Iraq (Markon, 2005b; Black, 2004).

Franklin was arrested in May 2005. At first, the press portrayed him as a cooperating player in the investigation, but by the fall, the FBI had decided that he was withholding information and they sought a superseding indictment. He pled guilty in early October 2005 to two counts of conspiracy to communicate national defense information to individuals not entitled to receive it (i.e., to Rosen and Weissman, both private American citizens, but not to an Israeli embassy official who also had been identified) and one count of unlawful retention of national defense information after a search revealed 83 classified documents in his home (United States District Court for the Eastern District of Virginia, Criminal complaint, 2005; Markon, 2005a).

Franklin was sentenced on January 20, 2006, to 151 months (12 years and 7 months) in prison and fined $10,000 (Johnston, 2006). In 2009, however, after the related case against the two AIPAC lobbyists was dropped, the judge reduced Franklin's sentence to probation with 10 months of community confinement and 100 hours of community service, specifying that the hours should be spent giving talks to audiences of young people on the rule of law (Markon, 2009; United States District Court for the Eastern District of Virginia, Motions hearing, 2009).

In 2005, the government indicted Rosen and Weissman and charged them with espionage on the grounds that they had conspired with Franklin to receive classified information, and then had passed it on to various members of the press

and to foreign officials.[41] This was an unusual prosecution, since Rosen and Weissman were not government employees and had no clearances. A key point in trial preparations was whether the information Franklin passed to them was national defense information (i.e., the language specified in the espionage statutes), and whether it actually was classified, since it had been delivered verbally. It was the first time civilians who were not working for and who had never worked for the U.S. government were prosecuted under the espionage statutes (Pincus, 2009).

The complex case against Rosen and Weissman dragged on for years, with the defense threatening to call prominent government officials as witnesses, and the government repeatedly filing motions to clarify the parameters of the trial. A reporter following the case noted, "U.S. District Judge T.S. Ellis III presided over 40 hearings on the matter, and he delivered 12 published decisions. Seven separate trial dates were set and postponed [over] 3 ½ years" (Pincus, 2009). Judge Ellis ruled that the prosecution would need to prove both that the defendants had acted "willfully," and that they had acted "with reason to believe it could be used to the injury of the United States or to the advantage of any foreign nation." Because the case involved verbally-transmitted information rather than actual documents, according to Judge Ellis, the case would come under 18 U.S.C. § 793(e), the subsection added in 1950 to raise the burden of proof on the communication of intangible information (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006). The government eventually dropped the case against Rosen and Weissman in May 2009, citing its concerns that classified information would be disclosed at trial and that the elements of proof required by the court made successful conviction unlikely (Markon, 2009).

The seven leakers discussed here were diverse. They ranged in age from 22 to 52 years of age: one person was 22, four persons were in their middle years (their 30s or 40s), and two persons were in their early 50s. They worked in various agencies: two were members of the military (U.S. Navy and U.S. Army); two were civilian federal employees, current or former (OSD and CIA); and three were contractors (two to the FBI, and one to DoS). They had reached different stages in their careers, from an Army Private First Class to people at mid-career to a respected senior defense policy specialist. Three common motives run through the seven cases.

- The leakers strongly objected to something they saw being done in the course of their work. Franklin, Diaz, Leibowitz, Kiriakou, and Manning each objected to government policies or actions that they observed, and they chose to intervene, usually by making their objections public by releasing classified information.

---

[41]Preparations for their trial stirred debate among legal scholars about whether such a prosecution represented a correct application of the espionage statutes, since it could be seen to threaten guarantees of freedom of speech and freedom of the press. The district court judge, T.S. Ellis, issued numerous memoranda leading up to the trial to clarify his assumptions, including *United States v. Rosen*, 445 F.Supp.2d 602, 643 (E.D. Va 2006). His reading of the precedents, however, remains operative only in the Eastern District of Virginia, leaving room for other interpretations by other judges of the complex espionage statutes (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006).

- The leakers enjoyed playing the role of expert. Franklin, Leibowitz, Kim, Kiriakou, and Sachtleben each sought out or responded to opportunities to share their expertise.
- The leakers wanted to help and saw themselves as helping. Diaz, Kim, and Manning, were, in their view, trying to help people they had befriended or with whom they sympathized.

To illustrate how leaks are a form of espionage in most ways, but not in every way, the elements of classic espionage discussed earlier are here applied to the actions of Franklin based on details are from his superseding indictment (United States District Court for the Eastern District of Virginia, 2005).

- A context of competition. Franklin's job was to monitor the hostile international relationship between the U.S. and Iran after its 1979 revolution. After 9/11, a debate simmered in Franklin's agency over preparations for the invasion of Iraq.
- Secret means. Franklin verbally conveyed highly classified information to recipients in meetings held in places where they were less likely to be observed.
- Goal is secrets. Rosen and Weissman sought out a well-placed contact in OSD who could provide them with information. Rosen is quoted as saying on the telephone "that he was excited to meet with a 'Pentagon guy' [Franklin] because this person was a 'real insider.'"
- Political, military, economic secrets. The classified information Franklin leaked to Rosen and Weissman included CIA internal reports on Middle Eastern countries, internal deliberations by federal officials, policy documents, and national intelligence concerning Al Qaeda and Iraq.
- Theft. Franklin was not accused of passing stolen documents to the recipients, only verbal information based on them. He was accused of stealing and taking home classified documents.
- Subterfuge and surveillance. Franklin, Rosen, and Weissman held their meetings at various restaurants, coffee shops, sports facilities, baseball games, and landmarks in the Washington, DC, area. In one instance, they met at Union Station, and conducted their conversations at three different restaurants.
- Illegality. Franklin was convicted of Title 18 U.S.C. § 793(d) and (e).
- Psychological toll. In July 2004, after the FBI explained the evidence and the likely consequences of a prison term on his family, Franklin took the FBI's bargain for leniency and wore a wire during subsequent conversations with Rosen and Weissman.

Franklin's case tracks with most of the elements of classic espionage. Some of Franklin's contacts were Israelis, but the two AIPAC lobbyists were American citizens. Applying these elements to the other six leak cases discussed earlier reinforces this conclusion: leaks differ from classic espionage mostly in that the

initial recipients typically are Americans, rather than foreign nations or their agents.

### Edward Snowden

Because so much attention already has been paid to Edward Snowden's actions, it is appropriate to conclude this discussion of leaks with him even though, as a fugitive, he has not been tried or convicted of any crimes. Snowden claims to have been inspired by Bradley Manning. Like Manning, Snowden received considerable support from Julian Assange at WikiLeaks. After watching what happened to Manning and to Thomas Drake, who was prosecuted for leaking National Security Agency (NSA) information until the case was dropped, however, Snowden admits that he saw the likely consequences of his actions and fled (Pincus, 2013; LaFraniere, 2013; Wilentz, 2014).

As a young man, Snowden parlayed his talent with computers into trusted information technology (IT) positions in the Intelligence Community—first with the CIA, and then with the NSA as a contractor with Dell and Booz Allen. The more he saw of the expanded surveillance and foreign intelligence gathering secretly taking place in these agencies after 9/11, the more disillusioned he became. Like Manning, he was offended by the use of torture in interrogations, and later the drone strikes against targeted individuals (Miller, 2013).[42] Snowden's access as a trusted systems administrator to a wide variety of programs, his use of web crawler software to extend his search for more documents, and his claim[43] that he needed to use others' passwords to do his job allowed him to download an estimated 1.7 million documents onto hard drives (Wilentz, 2014; Bamford, 2014; Sanger & Schmitt, 2014; Hosenball & Strobel, 2013).

Snowden stole this archive gradually, apparently beginning in April 2012. He imagined releasing information little by little to the press and from there, inevitably, to U.S. adversaries and the world. Starting in January 2013, he contacted several people with offers to leak information, including Glenn Greenwald, a commentator previously with *The Guardian* newspaper in London, and Laura Poitras, a documentary filmmaker. Together, they planned how to store and transfer the classified data, assuming NSA's surveillance capabilities would be trained on them. Julian Assange provided legal counsel and agreed to pay for Snowden's foreign travel and lodging. On May 20, 2013, Snowden left Hawaii where he lived and worked, and took his hard drives to Hong Kong accompanied by a WikiLeaks editor (Wilentz, 2014).

Snowden publicly announced his actions on July 9 in a videotaped interview with Greenwald published in *The Guardian* (Reitman, 2013). He portrayed himself as a whistleblower bent on warning the American public about the government's

---

[42] See Miller, 2013 for a comparison of Bradley Manning and Edward Snowden.
[43] Snowden disputes the claim by journalists that he tricked co-workers into using their passwords and public key infrastructure certificates, but the co-workers support the claim.

surreptitious theft of their Fourth Amendment rights. He claimed he leaked classified information so the public could know about and insist on reform of the intelligence surveillance programs being carried without oversight. He was quoted as explaining,

> My sole motive is to inform the public as to that which is done in their name and that which is done against them. . . I'm willing to sacrifice all of that [his previous life] because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building. (Greenwald, MacAskill, & Poitras, 2013)

For the next 6 weeks, Snowden lived in hotels, avoided authorities and the press, and sought asylum in any of several South American countries. From Hong Kong he flew to Moscow on June 23, but was stalled in the Sheremetyevo International Airport transit zone when the U.S. withdrew his passport (Osborn & Anishchuk, 2013). On August 1, 2013, Russia offered Snowden 1 year of temporary political asylum, and he left the airport for living quarters provided for him. His asylum extended to 3 years and was then renewed. He has continued to live outside Moscow, where he gives occasional interviews, writes opinion pieces, lives with his girlfriend, and appears to be negotiating his next steps (Myers, 2013).

Working from his archive secreted outside Russia with the help of his less-constrained supporters, for 2 years Snowden leaked stories published by various press and Internet sites. His stolen documents show wide-ranging programs that the NSA secretly put in place after 9/11 ostensibly to track potential terrorists. For example, the NSA had been collecting and storing American citizens' bulk domestic phone records, cooperating with Internet providers to collect bulk email records, and surveilling the communications of foreign governments. For years the Foreign Intelligence Surveillance Act court had been serially approving these activities in secret, following the legal procedure set up to handle classified requests for authorization. Other documents from Australian and British sources reveal the extent of allied cooperation with NSA's surveillance programs (Bamford, 2014; Shane, 2013b).

Snowden has been charged with theft of government property and two counts of espionage (Shane, 2013b). The audit of what Snowden took lasted for months. The intermittent and ongoing release of additional documents keeps the leak alive and it has taken time to work out the ramifications and reactions flowing from their publication (Ignatius, 2014). Three NSA employees had their security clearances suspended and were investigated for allowing Snowden to use their public key infrastructure certificates; one person resigned from the NSA (Nakashima, 2014).

Critics of Snowden point out that America's adversaries, including terrorist groups such as Al Qaeda, quickly changed their communications protocols in response to his leaks. Because of Snowden, the U.S. lost valuable intelligence capabilities that

had taken millions of dollars and years to build (Tsukayama, 2014). One critic blamed a Snowden leak for contributing to the rise of ISIS by warning its leaders off unencrypted email, which they stopped using (Harris, 2015). Other information leaked by Snowden demonstrated that, for years, Chinese hackers had been penetrating various defense programs such as the Joint Strike Fighter through cyber espionage, but ironically, it also showed that the NSA was detecting and tracking this penetration, and was planning electronic countermeasures—until the leak tipped off the Chinese (Gertz, 2015).

Evaluation of Snowden continues to evolve and he remains a wanted fugitive. His actions suggest that he hopes that with hindsight, and as the public reacts to the substance of his revelations, authorities will soften, the political climate will shift, and he will be able to strike a plea bargain and return home (Gertz, 2014). To some extent this shift has begun to happen. There has been vigorous public protest against the secret programs Snowden revealed. In May 2015, a federal appeals court declared that NSA's collection of Americans' bulk telephone records was illegal, and Congress later voted to discontinue the program of government collection and storage, instead proposing to keep these records accessible but in the hands of the telephone companies (Savage, 2015).

In response to Snowden's leak, there have been efforts to temper or discontinue other controversial programs, and a campaign has begun to demonstrate more transparency within the Intelligence Community. "The intelligence community is by design focused on keeping secrets rather than disclosing them," the Civil Liberties Protection Officer for the Director of National Intelligence is quoted as saying. "We have to figure out how we can work with our very dedicated work force to be transparent while they're keeping secrets" (Gerstein, 2015). An international conference of intelligence officials reported agreement among themselves that "Snowden—love him or hate him—has changed the landscape," and that even though the leaks had been "hugely damaging", going forward, there should be no secret laws, there should be stronger external controls over agencies, and those agencies should abjure techniques such as interrupting data flows or hacking into other agencies' internal networks (Campbell, 2015).

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

Federal law has anyone acting within the U.S. as an agent of a foreign government to register since shortly before the Second World War. Congress passed FARA in 1938 in response to concern about foreign governments surreptitiously spreading propaganda to advance their interests, while the American government and the public could not tell who was really behind it. The immediate provocation for the law came from agents for Nazi Germany, who were arguing in the U.S. press that the steps Germany was taking toward rearmament in the late 1930s were a positive development for America because they were the best way to block the "Communist peril" (Koerner, 2003).

At first, registrations of foreign agents went to DoS, but in 1942, this responsibility was shifted to the Attorney General, where it remains today (Executive Order 9176, 1942). FARA focuses on political actions by agents of foreign governments, including lobbying, advertising, public relations, and fundraising for "foreign principals". It excludes specified commercial activities and actions by acknowledged foreign officials and embassy personnel (Department of Justice, "Criminal Resource Manual," 2015). According to the DoJ FARA Registration Unit, FARA requires "periodic public disclosure [by agents] of their relationship with the foreign principal, as well as activities, receipts, and disbursements in support of those activities" (Department of Justice, National Security Division, 2015). The unit tracks all registrations, and reports on them semi-annually to Congress, also making its reports available online to the public.[44] The reports reveal the scale of influences on the U.S. government. They are organized by country, from Afghanistan to Vietnam, and they list: the names, addresses, and professions of each agent; the foreign government for which they do work; the activities they undertake; the total monies they received for their services in the past 6 months; and a description of any information they disseminated. The entire report is nearly 300 pages long; just the single-spaced list of names and organizations runs to 31 pages, and includes lobbying firms, tourism promoters, public relations companies, legal practices, and policy consultants (Department of Justice, Report of the Attorney General, 2014).

While FARA serves as the foundation for efforts to track agents of foreign governments, it is the related criminal statute focused on the non-political and illegal activities that concerns students of espionage—the 1938 Agents of Foreign Governments Act (AFGA) (Title 18 U.S.C. § 951). AFGA specifies the penalties for not complying with FARA, and is the statute most often used to prosecute intelligence gathering and other crimes by individuals acting in secret at the behest

[44] The semi-annual FARA reports to Congress are available at http://www.fara.gov/annualrpts.html

of or in support of a foreign government or official, although there are other laws that may be used as well.[45]

The AFGA is deceptively simple: anyone acting as an agent of a foreign government who does not register with the Attorney General shall be fined and/or imprisoned not more than 10 years. AFGA defines an agent of a foreign government as "an individual who agrees to operate within the United States subject to the direction or control of a foreign government or official," but it specifies several exceptions for various acknowledged foreign personnel (Title 18 U.S.C. § 951). Because it is so open-ended, it can be used by itself to prosecute a wide variety of activities that may be undertaken by an agent of a foreign government, or, as circumstances warrant, it can be used along with other statutes that criminalize conspiracy, aiding and abetting, and a range of substantive crimes, including many that are espionage-related. Although AFGA does not specify the types of acts themselves, they are better described in 50 U.S.C. § 1801, Definitions, under the chapter on

[45] See the listing at Department of Justice, National Security Division, Foreign Agents Registration Act, FARA Related Statutes, 2015, at http://www.fara.gov/rstatutes.html .

Foreign Intelligence Surveillance.[46] The elements of such acts include clandestine operations, intelligence gathering, illegality, sabotage, terrorism, false identity, and the international proliferation of weapons of mass destruction.

---

[46] The definitions provided in U.S.C. § 1801 of Chapter 36, Foreign Intelligence Surveillance, of Title 50, War and National Defense, provide more specific legal descriptions for the activities that come under the AFGA and that typically would be associated with espionage. They include: "As used in this subchapter:

(a) "Foreign power" means—

(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation thereof;
(5) a foreign-based political organization, not substantially composed of United States persons;
(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) "Agent of a foreign power" means—

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation thereof;
(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation thereof; or
(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation thereof for or on behalf of a foreign power; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)."

## Individuals Charged as Agents of a Foreign Government

An analysis of the 30 individuals who were charged and convicted under AFGA demonstrates the flexible interpretation available in these prosecutions. Table 16 lists the 30 persons by cohort and includes a number of additional variables.

**Table 16**
**Individuals Convicted as Agents of a Foreign Government**

| Name | Citizen-ship | Level of Clearance | Volunteer or Recruit | Recruit -ed by | Foreign Intelli-gence Service (FIS) member | Coded as Both Classic Espionage and as a Foreign Agent |
|---|---|---|---|---|---|---|
| **Began 1947-1979** | **12 individuals** | | | | | |
| Alvarez, Carlos | naturalized | none | recruit | FIS | | |
| Boyce, Christopher | native | TS/SCI | volunteer | | | both |
| Butenko, John | native | TS | recruit | FIS | | both |
| Chung, Dongfan | naturalized | S | recruit | FIS | | |
| Humphrey, Ronald | native | TS | volunteer | | | both |
| Johnson, Robert | native | TS | volunteer | | | both |
| Kadish, Ben-Ami | native | S | recruit | FIS | | |
| Lee, Andrew | native | none | volunteer | | | both |
| Rees, Norman | naturalized | none | volunteer | | | |
| Szabo, Zoltan | naturalized | TS | recruit | FIS | yes | both |
| Thompson, Robert | native | S | volunteer | | | both |
| Whalen, William | native | TS | recruit | FIS | | both |
| **Began 1980-1989** | **5 individuals** | | | | | |
| Ali, Amen | naturalized | none | volunteer | | | |
| Alvarez, Elsa | naturalized | none | recruit | FIS | | |
| Chiu, Rebecca | naturalized | none | recruit | FIS | | |
| Hall, James | native | TS/SCI | volunteer | | | both |
| Mak, Chi | naturalized | S | recruit | FIS | yes | |

ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

| Name | Citizen-ship | Level of Clearance | Volunteer or Recruit | Recruit-ed by | Foreign Intelli-gence Service (FIS) member | Coded as Both Classic Espionage and as a Foreign Agent |
|---|---|---|---|---|---|---|
| **Began 1990-2015** | **13 individuals** | | | | | |
| Alonso, Alejandro | native | none | volunteer | | yes | |
| Gari, George | native | none | recruit | FIS | yes | |
| Guerrero, Antonio | native | none | recruit | FIS | yes | both |
| Hernandez, Linda | native | none | recruit | FIS | yes | |
| Hernandez, Nilo | naturalized | none | recruit | FIS | yes | |
| Latchin, Sami | naturalized | none | recruit | FIS | yes | |
| Nicholson, Harold | native | TS/SCI | volunteer | | | both |
| Nicholson, Nathaniel | native | none | recruit | family | | |
| Santos, Joseph | naturalized | none | recruit | FIS | yes | |
| Shaaban, Shaaban | naturalized | none | volunteer | | | |
| Shemami, Najeb | naturalized | none | recruit | FIS | | |
| Soueid, Mohamad | naturalized | none | recruit | FIS | yes | |
| Yai, John | naturalized | none | recruit | FIS | yes | |

An initial look at Table 16 suggests that categorizing espionage-related offenders by whether they were prosecuted and convicted under AFGA is not a very revealing strategy. Some individuals listed in this table were native-born and some were naturalized citizens. Some held security clearances and had access to classified information, but many did not. Many were recruited, but 40% were volunteers. A common thread does run among recruits, however, in that all but one were recruited by a foreign intelligence service. Some were convicted under both AFGA and classic espionage, but two-thirds were convicted under AFGA without classic espionage charges.

Using Table 16 as a starting point, the three tables that follow reorganize the entries by filtering on several of the variables of interest. Table 17 presents the classic spies who also were convicted as foreign agents. Table 18 presents employees of foreign intelligence services who were convicted as foreign agents. Table 19 presents persons who were not convicted of classic espionage but who were convicted of being agents of foreign governments. For some in this third group, acting as a foreign agent was their only conviction, while for others it was one of several offenses.

## Classic Spies Who Were Also Convicted as Foreign Agents

Table 17 lists those convicted of both classic espionage and of acting as an agent of a foreign government by cohort. Most of them began their espionage in the period before 1979.

**Table 17**
**Individuals Convicted Both of Classic Espionage and as Agents of a Foreign Government**

| Name | Citizenship | Level of Clearance | Volunteer or Recruit | Recruited by | Foreign Intelligence Service (FIS) member |
|---|---|---|---|---|---|
| **Began 1947-1979 8 individuals** | | | | | |
| Boyce, Christopher | native | TS/SCI | volunteer | | |
| Butenko, John | native | TS | recruit | FIS | |
| Humphrey, Ronald | native | TS | volunteer | | |
| Johnson, Robert | native | TS | volunteer | | |
| Lee, Andrew | native | none | volunteer | | |
| Szabo, Zoltan | naturalized | TS | recruit | FIS | yes |
| Thompson, Robert | native | S | volunteer | | |
| Whalen, William | native | TS | recruit | FIS | |
| **Began 1980-1989 1 individual** | | | | | |
| Hall, James | native | TS/SCI | volunteer | | |
| **Began 1990-2014 2 individuals** | | | | | |
| Guerrero, Antonio | native | none | recruit | FIS | yes |
| Nicholson, Harold | native | TS/SCI | volunteer | | |

Among the 11 individuals in Table 17, only Antonio Guerrero had no access to classified information. Guerrero was one of a group of people known as *La Red Avispa* (The Wasp Network, in Spanish) who were surveilling and gathering intelligence for the Cuban Intelligence Service (CIS) in south Florida during the 1990s. Ten network members were rolled up starting in 1998. Espionage charges were dropped for those who pled guilty to being foreign agents, and they received prison terms of 3 to 7 years. Guerrero, however, who had been born in Miami but was taken to Cuba as an infant, chose to go to trial.

The trial was held in Miami, where anti-Castro feeling ran high. In 2001, Guerrero was convicted of espionage as well as of being a foreign agent, and was sentenced to life in prison. His sentence was reduced to 21 years and 10 months in 2009 (Weaver, 2009). Recently, he was one of five Cubans and Cuban-Americans released to Cuba as part of the warming of diplomatic relations (Robles & Davis, 2014; Freeman, 2014).

Ten of the 11 individuals in Table 17 were native-born citizens. Seven of the 11 volunteered to commit espionage. Guerrero was one of four recruits in this group, all of whom were recruited by a foreign intelligence service. Two actually worked for an intelligence service as employees. Guerrero was one of these, as was Zoltan Szabo.

Szabo had served in the U.S. Army during the Vietnam War, and began working for the Hungarian intelligence service in 1967. He recruited Clyde Conrad, a retired American Army sergeant working at a military archives in Germany, who in turn recruited at least five of his Army confederates to be spies in his own espionage ring, first in West Germany and then in the U.S. The Conrad ring betrayed damaging intelligence on CIA sources and methods in Germany, and also nuclear secrets, including American plans in the event of nuclear war with the Soviets. Szabo cooperated with investigators against Conrad in exchange for a light sentence. He was tried in Austria rather than in the U.S. and received no prison time (Gerth, 1989; Rafalko, n.d.).

### Employees of Foreign Intelligence Services

Table 18 lists those who worked directly for a foreign intelligence service and who were convicted of acting as an agent of a foreign government. Seven of the 11 were naturalized citizens. Ten of the 11 were recruited by their foreign intelligence service; only one volunteered. Unlike the nine people in the most recent cohort, the two individuals who began espionage before 1990, one in each of the two earlier cohorts, held security clearances. Only Szabo is coded as both an instance of classic espionage and acting as an agent of a foreign government.

**Table 18**
**Individuals Working for a Foreign Intelligence Service (FIS) and Convicted as Agents of a Foreign Government**

| Name | Citizenship | Level of Clear-ance | Volunteer or Recruit | Recruit-ed by | Foreign Intelligence Service (FIS) member | Coded as Both Classic Espionage and as a Foreign Agent |
|---|---|---|---|---|---|---|
| **Began 1947-1979** | **1 individual** | | | | | |
| Szabo, Zoltan | naturalized | TS | recruit | FIS | yes | both (imputed) |
| **Began 1980-1989** | **1 individual** | | | | | |
| Mak, Chi | naturalized | S | recruit | FIS | yes | |
| **Began 1990-2015** | **9 individuals** | | | | | |
| Alonso, Alejandro | native | none | volunteer | | yes | |
| Gari, George | native | none | recruit | FIS | yes | |
| Guerrero, Antonio | native | none | recruit | FIS | yes | both |
| Hernandez, Linda | native | none | recruit | FIS | yes | |
| Hernandez, Nilo | naturalized | none | recruit | FIS | yes | |
| Latchin, Sami | naturalized | none | recruit | FIS | yes | |
| Santos, Joseph | naturalized | none | recruit | FIS | yes | |
| Soueid, Mohamad | naturalized | none | recruit | FIS | yes | |
| Yai, John | naturalized | none | recruit | FIS | yes | |

If there is a trend in Table 18, it is the reverse of the one noted in Table 17; 82% began their espionage in the most recent cohort, in contrast to the classic spies in Table 17 who most frequently began in the earliest cohort. Since 1990, several things could be happening to cause this trend. Perhaps there are more employees of foreign intelligence services spying in the U.S. than there have been in the earlier periods. A former head of the House Intelligence Committee, Mike Rogers, suggested this when he publicly claimed in April 2016, "There are more spies in the United States today from foreign nation-states than at any time in our history—including the Cold War, and they're stealing everything. If it's not bolted down, it's gone" (Hattem, 2016). Then again, perhaps more of them are being caught, prosecuted, and convicted on the charge of serving as agents of a foreign government.

### Persons Not Convicted of Classic Espionage, but Convicted of Acting as Agents of Foreign Governments, Solely or with Other Charges

Table 19 lists the 19 individuals prosecuted for acting as agents of a foreign government. Nine of the 11 employees of foreign intelligence services appear both in Table 18 and in Table 19. Employees of foreign intelligence services sent to become U.S. naturalized citizens, and thereby become eligible to gain positions with access to classified information, typically are acting as agents of the government that sent them.

A trend seems to be strengthening to use AFGA alone to prosecute American citizens who work for foreign intelligence services. In the recent past, there have been more successful prosecutions using this statute than there were in past cohorts. However, not all of the individuals solely charged and convicted under AFGA fit this pattern. Ben-Ami Kadish, for example, began espionage during the earliest cohort and only was charged as a foreign agent.

Also, not all of the known employees of foreign intelligence services who committed espionage, and who are included in this study, were charged with acting as a foreign agent, although obviously they did so. At least three such employees were charged and convicted only of classic espionage. This underlines the discretion prosecutors may exercise and the effect of circumstances and context in each case of espionage.

**Table 19**
**Individuals Not Convicted of Classic Espionage but Convicted as Agents of a Foreign Government**

| Name | Citizenship | Level of Clear-ance | Volunteer or Recruit | Recruit-ed by | Foreign Intelligence Service (FIS) member | Convicted Only as Acting as a Foreign Agent (FA) |
|---|---|---|---|---|---|---|
| **Began 1947-1979 4 individuals** | | | | | | |
| Alvarez, Carlos | naturalized | none | recruit | FIS | | Only FA |
| Chung, Dongfan | naturalized | S | recruit | FIS | | |
| Kadish, Ben-Ami | native | S | recruit | FIS | | Only FA |
| Rees, Norman | naturalized | none | volunteer | | | Suicide, not tried |
| **Began 1980-1989 4 individuals** | | | | | | |
| Ali, Amen | naturalized | none | volunteer | | | |
| Alvarez, Elsa | naturalized | none | recruit | FIS | | Only FA |
| Chiu, Rebecca | naturalized | none | recruit | FIS | | Only FA |
| Mak, Chi | naturalized | S | recruit | FIS | yes | |
| **Began 1990-2015 11 individuals** | | | | | | |
| Alonso, Alejandro | native | none | volunteer | | yes | Only FA |
| Gari, George | native | none | recruit | FIS | yes | Only FA |
| Hernandez, Linda | native | none | recruit | FIS | yes | Only FA |
| Hernandez, Nilo | naturalized | none | recruit | FIS | yes | Only FA |
| Latchin, Sami | naturalized | none | recruit | FIS | yes | |
| Nicholson, Nathaniel | native | none | recruit | family | | |
| Santos, Joseph | naturalized | none | recruit | FIS | yes | Only FA |
| Shaaban, Shaaban | naturalized | none | volunteer | | | |
| Shemami, Najeb | naturalized | none | recruit | FIS | | |
| Soueid, Mohamad | naturalized | none | recruit | FIS | yes | |
| Yai, John | naturalized | none | recruit | FIS | yes | Only FA |

Larry Wu-tai Chin joined the intelligence service in China in the 1940s and came to the U.S. tasked with collecting intelligence. He became an American citizen, an analyst, and a translator for the CIA, all the while spying for China. Over his 30-year spying career, Chin earned a salary from China that may have approached $1 million, and he grew wealthier still by buying investment properties around Washington, DC. He supported a gambling habit that was so severe that several Las Vegas casinos cut off his access. Chin transmitted closely-held secrets on American Far East policy for decades, starting with reports on American interrogations of Chinese prisoners during the Korean War. After his conviction in February 1986 on all 17 counts of espionage with which he had been charged, he committed suicide in his cell (Engelberg, 1986).[47]

Karl Koecher joined the Czechoslovak foreign intelligence service in 1963 and spent 2 years in intelligence training, after which he was sent to the U.S. with his wife and fellow agent, Hana Koecher.[48] They became naturalized citizens, and Karl taught philosophy at a Staten Island college for 4 years. In 1973, he obtained a security clearance and took a job as a contract translator for the CIA. From 1975 to 1977, he worked as a CIA employee and spied for the Czechs, but in 1977, he lost his CIA job and returned to teaching. Hana got a job in the diamond trade in New York City, and worked as a courier, moving information to the Czechs until the Koechers were arrested in November 1984. Two years later, they were exchanged for Anatoly Shcharansky, a famous Russian dissident. They returned to Czechoslovakia, where the government welcomed them as heroes and granted them use of a villa outside Prague and a new Volvo (Raab, 1984; Stein, 2010).

Ali Mohamed, a former Egyptian military officer, enlisted in the U.S. Army in 1986, became an American citizen by marrying an American woman, and served as a cultural and military advisor for the Army during the late 1980s and then for the FBI during the 1990s. While playing the role of U.S. cultural asset, however, Mohamed actually was a committed Islamic extremist working for Ayman al-Zawahiri. He took leave from the Army in 1988 and spent several weeks fighting with the Mujahedeen in Afghanistan. Despite critical reports from his superior officers, he received no formal punishment from the Army and the Intelligence Community took no action. Then, in 1989, Mohamed began traveling from his Army base to New York City where he advised Islamic radicals, including the group that would bomb the World Trade Center in 1993. He also used Army manuals that were classified Secret to produce a textbook for Al Qaeda trainees on collecting intelligence, doing surveillance, and planning terror attacks.

Mohamed resigned from the Army in 1989, and left with an honorable discharge in

---

[47] Reports on Chin's death stated that he committed suicide by putting a plastic bag over his head and tying it with his shoelaces (Engelberg, 1986).

[48] Hana Koecher was not charged with espionage or being a foreign agent, but of misprision, that is, concealment of a felony committed by her husband. She is not included as one of the individuals coded in this study.

1991. Zawahiri then asked him to coordinate the move of Bin Laden's family and its supporters from Afghanistan to Sudan. During the late 1990s, Mohamed worked directly for Bin Laden and Al Qaeda. His tasks included providing military training—learned from the U.S. Army—to Al Qaeda recruits and scouting the U.S. embassy in Nairobi, one of the two American embassies in East Africa that Al Qaeda bombed.

Mohamed was arrested after the East Africa bombings in September 1998 and pled guilty to five charges of terrorism and falsification. He then remained in prison for months without being sentenced, and eventually, he dropped out of public view and disappeared (Weiser & Risen, 1998; Williams & McCormick, 2001; Poole, 2010).

Fourteen of the 19 people in Table 19 were naturalized citizens. Of the 11 persons who began activities in the most recent cohort, none held a security clearance, and only three had clearances in the previous two cohorts. Fifteen were recruited and four were volunteers. Of the recruits, only Nathaniel Nicholson was not recruited by a foreign intelligence service, but instead, by his father.

Norman Rees,[49] listed in Table 19 as having committed suicide before he could be tried, was unusual because his espionage lasted so long. He worked as a petroleum engineer and began sharing unclassified information about the oil industry with the Soviets in 1942, when the U.S. and the Soviet Union were allies. Sympathetic toward Communism, as World War II ended and the Cold War began and intensified, Rees continued to collect and pass American industrial information and techniques to the Soviets until 1971, when the FBI interviewed him. At that time, Rees agreed to work for them as a double agent. In 1976, when he learned that a Dallas newspaper was about to publish his story and name him, Rees committed suicide (Blau, 1976).

Rees' information had been so valuable to the Soviets that they paid him $30,000 along with a $5,000 annual pension. He received a medal for the valuable catalytic cracking converter equipment he passed to the Soviets in 1950, which set the subsequent course of Soviet oil industry development (Associated Press, 1976).

Of the 10 persons in Table 19 who were convicted solely of being foreign agents, seven of them were working with the CIS, all in south Florida. Carlos and Elsa Alvarez, both naturalized American citizens, had been working separately for the Cubans when they met and married in the early 1980s. Carlos Alvarez taught psychology at Florida International University (FIU) and began passing information to the Cubans in 1977 until 2005. As a professor, Carlos made repeated trips to Cuba with his FIU students to introduce them to the island and to foster friendly attitudes between the two countries. Elsa Alvarez also worked at FIU as a counselor and began spying in 1982. They were arrested in 2006 and convicted in March

[49] Norman Rees is included in the PERSEREC Espionage Database because of his long career despite having begun espionage in 1942. What he would have been charged with has been imputed.

2007 of conspiracy to act as agents of a foreign government (United States District Court Southern District of Florida, 2007; Weaver, 2007).

The Alvarezes wrote reports that they encrypted onto computer disks and sent to the CIS via post office boxes in New York City. They used code names, a short wave radio, messages on water-soluble paper, coded pager messages, and personal meetings in Cuba to receive instructions for their surveillance and collection. Cuban intelligence wanted information on any prominent people the Alvarezes knew or could find out about, attitudes in the south Florida community, political developments as they might affect Cuba, and current events of concern to the Cuban government. Carlos was sentenced to 5 years in prison, while Elsa received 21 months (1 year and 9 months) (United States District Court Southern District of Florida, 2007).

The other five individuals convicted solely of being foreign agents for Cuba were part of *La Red Avispa*. Alejandro Alonso, George Gari, Linda and Nilo Hernandez, and Joseph Santos all pleaded guilty in 1999 and 2000 to acting as agents of a foreign government and served various prison terms between 4 and 7 years.[50] The network's agents infiltrated anti-Castro immigrant groups to report on their plans, and took jobs at military bases in south Florida where they surveilled and reported on activities. Although they hoped to gain access to classified information, none did (Pressley, 1998; "Miami Spy-hunting, 2000).

Five of the persons listed in Table 19 supplied information or equipment to Middle Eastern countries. Two were volunteers, Amen Ali and Shabaan Shabaan, and three were recruits by foreign intelligence services. Sami Latchin and Najib Shemami were recruited to work for Iraq, and Mohamad Anas Haitham Soueid was a recruit for Syria. All five were convicted of export control or trade embargo offenses along with acting as an agent of a foreign power. Ali, for example, tried to ship dual-use military equipment to Yemen (Kotowski, 2011), while Shabaan worked with the Iraqi Intelligence Service (IIS) and collected open source intelligence on American intentions during the run-up to the Iraq War (Corcoran, 2006).

Latchin came to the U.S. in 1993 on orders from Saddam Hussein to fit in, become a citizen, and collect information on Iraqi opposition groups. While a sleeper, however, Latchin slowly spent his way into bankruptcy and was working as a gate agent at O'Hare Airport when he was arrested. He had been identified in 2004 in documents that had been captured in Iraq, and he was convicted in 2007 of being a foreign agent, violating the trade embargo against Iraq, and various falsifications (Coen, 2007).

Like Latchin, Shemami and Soueid are examples of foreign agents who had no access to classified or restricted information, but who instead focused on surveilling immigrant communities and sending reports to foreign governments that were

[50] Others in the network who were not American citizens are not included here.

worried about the threat these communities could pose to their regimes. Shemami was a naturalized citizen who had lived in the Detroit, Michigan area for some 40 years when he was arrested in 2007 and initially charged with four espionage-related offenses, including acting as an unregistered foreign agent. Like Latchin, his indictment was based on Iraqi intelligence records captured during the Iraq War ("Community members spied for Iraq," 2007).

Starting in September 2002 through January 2003, Shemami worked for the IIS collecting and reporting observations and information he gathered from his community in Detroit and during three trips he made to Iraq and Turkey. As a merchant and importer, Shemami had traveled frequently to and from the Middle East since 1996. While the U.S. prepared for a likely invasion of Iraq in 2002, the IIS recruited him as an agent by making him a deal: he could continue importing foodstuffs[51] unhindered by the Iraqi authorities in exchange for information the IIS requested (Associated Press, 2009).

The captured IIS records documented Shemami's contributions to Saddam Hussein's regime, including: naming Iraqi natives living in the U.S. whom Shemami judged would be asked to guide American troops during an invasion of Iraq; names of expatriates who could become potential political candidates in Iraq; observations he made of military preparations in Turkey, such as the locations of 200 tanks and tents made ready for refugees; and the name of an Iraqi expatriate interviewed by, and possibly cooperating with, the FBI (United States District Court Eastern District of Michigan, 2007; Ashenfelter, 2007).

Shemami would be among the first of a dozen Iraqis in the U.S., both naturalized citizens and permanent residents, prosecuted in the late 2000s for acting as agents of Saddam Hussein's government based on captured records. Hussein had maintained an extensive operation. He watched for threats to his regime in the U.S., and gathered intelligence by sending in sleeper agents who were directed to live quietly and blend into American society until instructed by the IIS to collect specific information (Leinwand, 2008).

Shemami was charged with conspiracy to act as an unregistered agent of a foreign government, acting as such an agent, providing services to Iraq in violation of the International Emergency Economic Powers Act (IEEPA), and lying to the FBI (United States District Court Eastern District of Michigan, 2007). His defense argued at trial that the IIS had coerced him into becoming an agent by threatening him with torture. One Detroit FBI agent refuted that claim and said help was available to resist such pressure. "We're here to help them. . . . There are ways we can help them. They also have to say 'Hey, we need help'" (Egan, 2009). Shemami pled guilty early in 2009 and was sentenced to 46 months (3 years and 10 months) in prison, leaving behind a wife and nine children (Schmitt, 2009).

---

[51] Some observers said he smuggled goods and medicine back into Iraq as well.

## ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

The regime of Bashar al-Assad, President of Syria, also was declared a threat to the national security of the U.S. under IEEPA based on its state support for terrorism. Similar to Saddam Hussein, Assad has run American agents to observe and to report names and threatening activities among disaffected Syrian expatriates in the U.S. Soueid, a Syrian-born naturalized American citizen living in Leesburg, Virginia, was arrested on October 11, 2011, and charged with conspiring to and actually acting as an agent of a foreign government, and with four counts of lying on firearms forms and to federal agents (United States Department of Justice, 2011).

As the protest movement in Syria against Assad escalated in 2011, Soueid helped monitor protestors among the Syrian immigrant communities in the U.S. Soueid also recruited others to record audio and video at anti-Assad public protests, and to make recordings of conversations with participants that could be used later by the Syrian intelligence service for identification purposes. He passed along phone numbers and email addresses of protest leaders, details about individuals who were financing the protests, logistics of meetings, internal conflicts developing within the movement, and its future plans, along with dozens of audio and video recordings. He traveled to Syria several times between March and October 2011, where he met personally with Assad (United States Department of Justice, 2012; United States Department of Justice, 2011; Goodman, 2011). He used a laptop computer provided by Syrian intelligence to communicate securely with his contacts in the Syrian embassy in New York and in Syria. He destroyed the laptop and burned documents in his backyard after an interview with the FBI implied his imminent arrest.

Soueid was convicted in March 2012 of acting as an unregistered government agent and of falsification, and was sentenced the following July to 18 months in prison and 3 years of probation. He claimed at his trial that he was acting to prevent Islamic extremists from taking over Syria, who in turn would create a larger national security threat to the U.S. than Assad ever had (Associated Press, 2012). "By illegally acting as an agent of Syria, Mr. Soueid deceived his adopted country of the United States in support of a violent and repressive despotic regime," the FBI Assistant Director said at his sentencing. "Through today's sentencing, he will now be held accountable for his actions" (United States Department of Justice, 2012).

Acting as an agent of a foreign government is, in a large sense, the essence of espionage. Applying the categories from the discussion of classic espionage earlier to the example of Soueid's actions helps to demonstrate how being a foreign agent is like, but not completely like, the classic pattern:

- A context of competition. Syria has been designated a state sponsor of international terrorism by DoS since 1979, and various economic, financial, and trade sanctions have been imposed based on that designation.
- Secret means. Soueid and his co-conspirators secretly made audio and video recordings of opponents of the Assad government in the U.S. and emailed the

recordings to the Syrian intelligence service so its agents could identify and take punitive action.

- Goal is secrets. No classified or restricted information was involved in Soueid's case. Instead, he collected the identities (e.g., names, addresses, and email addresses) of Syrian opponents of Assad, and recorded their political protests for Syrian intelligence.
- Political, military, economic secrets. The secrets that Soueid collected were the political opinions of individual protesters and the political plans that groups made to protest and act against the regime. Soueid was sued in a civil action by several people whose lives had been damaged as a result of his surveillance, including one woman whose father was murdered in Syria and whose daughter had been kidnapped.
- Theft. The theft done by Soueid and his co-conspirators was theft of the privacy and security of the Syrian legal residents of the U.S. who were lawfully assembling and expressing their views in peaceful protest.
- Subterfuge and surveillance. Soueid and his co-conspirators clandestinely attended protest rallies and planning meetings of groups opposed to Assad, secretly made recordings, and lied to the FBI about their actions.
- Illegality. Soueid was charged with Title 18 U.S.C. § 371, conspiracy to act as an agent of a foreign government, Title 18 U.S.C. § 951, acting as an agent of a foreign government, Title 18 U.S.C. § 922(a)(6), material false statement on a firearms purchase application, Title 18 U.S.C. § 924(a)(1)(A), false statement on a firearms application, and Title 18 U.S.C. § 1001, false statements to the FBI. He was convicted of conspiracy to act and of actually acting as an agent of a foreign government and of various falsifications.
- Psychological toll. After the FBI interviewed him but before he was arrested, Soueid burned some of his documents in his backyard and destroyed the laptop computer given to him by Syrian intelligence, suggesting that he was anxious about the legal consequences of being caught. During his trial, however, he continued to be defiant in his support for the Assad regime (United States Department of State, 2015; United States District Court for the Eastern District of Virginia, Alexandria Division, Indictment, 2011; Department of Justice, Office of Public Affairs, 2012).

As the examples of Soueid and the others discussed in this section illustrate, the statutes that define acting as an agent of a foreign government are general and do not name espionage itself, yet the acts of such agents, even when they do not have access to classified or controlled information, play out an espionage scenario.

ACTING AS AN AGENT OF A FOREIGN GOVERNMENT AS A TYPE OF ESPIONAGE

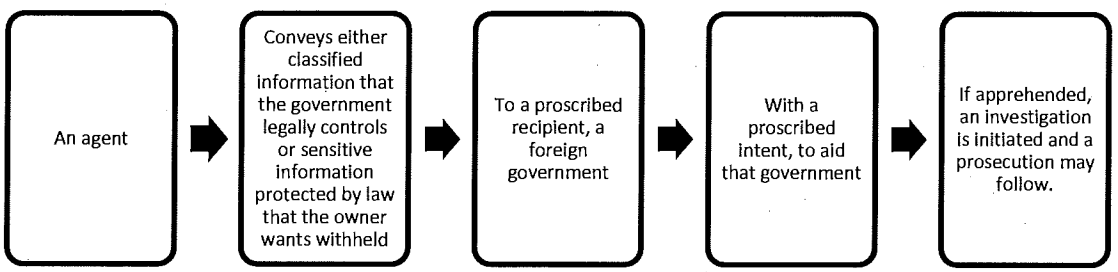



**Figure 5 Acting as an Agent of a Foreign Government in a Model of Espionage Elements**

In the U.S., such agents collect information and clandestinely pass the information to a foreign government, thereby causing damage to the U.S. In some instances, the damage is to the interests or people of expatriate communities, in others by meddling in American foreign policies, economic developments, or international military actions (Koerner, 2003). In the cases of Shemami and Soueid, they brought the wars in Iraq and Syria into their immigrant communities at home in America. They served as agents of foreign governments, but they were also American citizens who betrayed their allegiance to the U.S.

## VIOLATIONS OF EXPORT CONTROL LAWS AS A TYPE OF ESPIONAGE

The U.S. considers the sale, export, or re-transfer of various American defense articles and knowledge to be potential threats to its national security, its economic security, and its foreign policy goals. These defense articles include: military technology; dual-use technologies and software; defense services; conventional weapons; missile technology; satellites; and nuclear, chemical, or biological materials and/or weapons. Together, they constitute millions of items (United States Department of State, Directorate of Defense Trade Controls, 2015a).

Legislation to counter these threats by controlling exports of these sensitive items originated in times when the U.S. was facing war, with laws such as the Trading with the Enemy Act of 1917 and the Neutrality Act of 1935. Congress considered these laws necessary to prevent "giving aid and comfort to the nation's enemies" when, as war approached, it was clear who those enemies would be (Fergusson, 2009). In the late 1940s, as the Cold War took hold, controlling defense exports shifted from its initial wartime focus to one of preventing the Soviets and their allies from procuring articles, knowledge, and/or materials that would help them if an actual war broke out. Export control grew to become an extensive and complex federal enterprise, designed to be carried on indefinitely (Fergusson, 2009; Fergusson & Kerr, 2014).

The mechanisms of export control available to regulators in the 1950s (i.e., lists of proscribed items, procedures to license approved exports and deny licenses to those that are disapproved) shaped the export control system that persists today. The assumptions derived from the context of the 1950s—that of a face-off between two super powers—also shaped the system. Yet, since then, the world has become a different place, one that is more globalized, more internationally interconnected, and one in which the U.S. faces multiple competitors and potential adversaries.

For years, people have argued that the export control system needs large-scale revision to bring it up to date. Critics do not agree, however, on how it should be revised. Some argue for loosening controls to boost trade and economic profit, thereby benefiting the American economy. Others argue for tightening export controls to hold on to America's technological advantages in the face of accelerating international competition.

Two main federal agencies handle licensing of controlled exports: DoS and the Department of Commerce (DoC).[52] Due to inadequate coordination between them, disputes over their respective jurisdictions, and vexing delays for applicants, the Government Accountability Office (GAO) in 2007 declared export control to be a high risk area that required strategic reexamination. In response, the Obama Administration began a major revision of the system in 2009, working to simplify and unite it by designating: one licensing agency instead of the two main and many subsidiary agencies; one list of items that require an export license, instead of the two overlapping lists now in place; one enforcement structure; and one IT system that all users could access (Levine, 2012; Fergusson & Kerr, 2014). As of 2015, reformers were making slow but appreciable progress, starting with steps to cross-reference and reconcile the two lists.

### Three Export Control Statutes

The three main statutes governing export control all date from the late 1970s. Their authors made use of the procedures then available that had built up since the First World War. These three statutes now define the current export control system, with some later revisions.

The Export Administration Act (EAA) of 1979[53] controls dual-use technologies, that is, technologies that may have both commercial and military uses. It is implemented by DoC through the Export Administration Regulations (EAR).[54] The list of specific items tracked under the EAR, which require export licenses from DoC, is called the Commerce Control List (CCL). There are 10 broad categories on the CCL:

- Nuclear materials, facilities, and equipment;
- Materials, chemicals, microorganisms, and toxins;
- Materials processing;
- Electronics design development and production;
- Computers;
- Telecommunications and information security;
- Lasers and sensors;

---

[52] This discussion simplifies a complicated regulatory landscape. Numerous federal agencies have roles in regulating specific exports, such as the Department of Energy and the Nuclear Regulatory Commission, which deal with various aspects of nuclear weaponry and materials. DoD also plays an important role in defining military weapons, articles, and technology of all types and overseeing their global availability. The Bureau of Industry and Security, which administers export control in DoC, lists sections of nine federal agencies that have responsibilities for export control. In addition to those already mentioned here, the list includes the Department of the Interior, the Drug Enforcement Administration, the Food and Drug Administration, the Patent and Trademark Office, and the Environmental Protection Agency. (See http://www.bis.doc.gov/index/php/about-bis/resource-links)

[53] Title 2 of P.L. 96-72

[54] 15 C.F.R. 730 et seq.

- Navigation and avionics;
- Marine; and
- Aerospace, propulsion systems, space vehicles, and related equipment (Fergusson, 2014).

According to a 2014 Congressional Research Service report,

> Each of these categories [that are listed on the CCL] is further divided into functional groups: equipment, assemblies, and components; test, inspection, and production equipment; materials; software; and technology. Each controlled item has an export control classification number (ECCN) based on the earlier categories and functional groups. Each ECCN is accompanied by a description of the item and the reason for control. In addition to discrete items on the CCL, nearly all U.S.-origin items are 'subject to the EAR.' This means that any item 'subject to the EAR' may be restricted to a destination based on the end-use or end-user of the product. For example, a commodity that is not on the CCL may be denied [a license to export] if the good is destined for a military end-use or an entity known to be engaged in weapons proliferation. (Fergusson, 2014)

Oddly, Congress has repeatedly allowed the 1979 EAA to expire, and then turned around and renewed it for a specified period of time. During periods when it is expired, as it was in 2015, successive presidents have declared that all of its powers and requirements will continue under the authority granted to the president under the IEEPA, discussed further.

The second major statute is the Arms Export Control Act (AECA) of 1976,[55] which regulates military technology. It requires the president to control the import and export of defense articles and services, which include consulting, advising, and sharing information. This sharing is one of the activities that can lead to charges of espionage. The AECA requires that governments that receive or buy weapons and other military items from the U.S. use them for internal security and legitimate self-defense, not for aggression or escalation of a conflict. Elements that are considered in determining the legitimacy of an export include whether the exports contribute to an arms race, if they aid in the development of weapons of mass destruction, or if they support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements (Fergusson & Kerr, 2014).

The AECA is implemented by DoS through ITAR.[56] The list of specific items tracked under ITAR, which require export licenses from DoS, is called the U.S. Munitions List (USML). There are 21 broad categories on the USML, including:

---

[55]Title 2 of P.L. 94-329, 90 Stat. 729, enacted June 30, 1976, codified at 22 U.S.C. chap. 39.
[56] C.F.R. 120-130.

- Firearms, Close Assault Weapons and Combat Shotguns;
- Guns and Armament;
- Ammunition/Ordnance;
- Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines;
- Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents;
- Surface Vessels of War and Special Naval Equipment;
- Ground Vehicles;
- Aircraft and Related Articles;
- Military Training Equipment and Training;
- Personal Protective Equipment;
- Military Electronics;
- Fire Control, Range Finder, Optical and Guidance and Control Equipment;
- Materials and Miscellaneous Articles;
- Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment;
- Spacecraft and Related Articles;
- Nuclear Weapons Related Articles;
- Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated;
- Directed Energy Weapons;
- Gas Turbine Engines and Associated Equipment;
- Submersible Vessels and Related Articles; and
- Articles, Technical Data, and Defense Services Not Otherwise Enumerated. (Department of State, Directorate of Defense Trade Controls, 2015b)

A glance through the categories on DoC's CCL followed by DoS's USML suggests the potential for disagreement and likely confusion for those applicants who deal with both agencies. For instance, the lists overlap, they use different terms for the same or similar items, and their categories do not match. This is why the export control reform effort decided that the first project it would take on was to reconcile the two lists.

The third major export control statute is the IEEPA of 1977,[57] which grants the president the ability to declare an emergency when the U.S. is under unusual and extraordinary threat from abroad, short of war. Under such an emergency, the president may block financial transactions or freeze assets of belligerent foreign

[57] Title 2 of P.L. 95-223.

governments or specific foreign nationals. President Carter first declared an IEEPA emergency in 1979 in response to the Iran hostage crisis, and Iranian assets continued to be frozen by sanctions until early 2016 when a nuclear deal was reached (Pearce, 2016). When DoS declared Syria to be a state sponsor of terrorism in 2004, the U.S. froze its assets under IEEPA. Emergencies such as the 9/11 attacks caused a similar blocking of Al Qaeda's assets and freezing of its finances in the U.S. (Fergusson & Kerr, 2014).

These statutes from the 1970s are sometimes insufficient to address 21st century national and economic security demands. For example, a larger proportion of sensitive technology is now dual-use, and thus, requires a difficult assessment by export control regulators of the risk that what is bought as a commercial application might be diverted to a military end use. Second, more countries are exporting sensitive dual-use technologies, including newer arms suppliers like China, Israel, Turkey, and Ukraine. Third, globalized methods of manufacturing now result in sensitive dual-use technologies becoming international (i.e., a defense article can be financed in one country, designed in a second, and assembled in a third). Fourth, sensitive technologies have spread around the globe and are no longer the special province of just a few advanced countries, so it becomes complicated to track and "maintain sovereignty" over those technologies. Fifth, with more competition among international arms suppliers, it becomes difficult to exert discipline on exporters to deny them business. That is, if an international customer is blocked from buying what it wants from the U.S., it can turn around and buy it from another country. Finally, the health of the economy may now be more intertwined with national security than it ever has been, making access to international markets not simply a commercial goal, but one that has direct implications for U.S. security (Beck, 2000).

### Enforcement of Export Control

Enforcement of export control statutes is, in large part, the responsibility of the Counterintelligence and Export Control Section (CES) in DoJ's NSD, the same legal section that handles enforcement of FARA. According to its website,

> the CES supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology. The Section has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. (United States Department of Justice, "Counterproliferation overview," 2015)

Putting the response to export control violations in the counterintelligence section of DoJ's NSD demonstrates the federal government's appreciation that these violations endanger national security as well as the country's economic advantages. When people illegally export military technology, a dual-use article, or information

that falls under export control, they commit espionage in impact if not currently in name. The model that illustrated classic espionage earlier in this report also can illustrate the basic elements of export control violations.

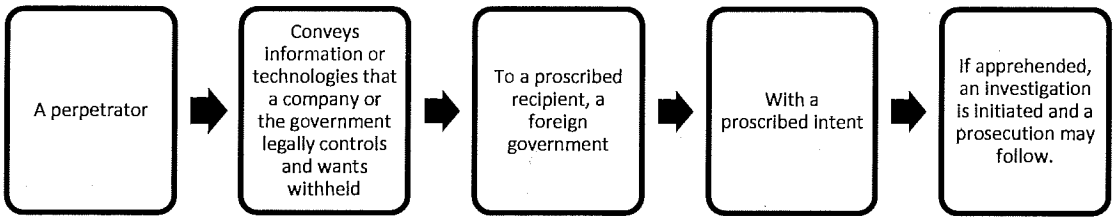



**Figure 6 Export Control Violations in a Model of Elements of Espionage**

In Figure 6, proscribed recipients of controlled exports would include countries specified by name under declared IEEPA emergencies that continue in place, including Syria, North Korea, and Lebanon. Other proscribed countries are listed by the various regulatory agencies that publish lists of specific denied exports or that fall under general trade sanctions. Lists include the DoS "U.S Embargo Reference Chart" and the DoC "Denied Persons List" and "Entity List." China, Iraq, Libya, Syria, Sudan, and many others are on these lists. Some defense items are proscribed for export to virtually any foreign government. Proscribed intent is specified in the three statutes governing export control under discussion here, which criminalize transferring controlled items or information without the evaluation of regulators and their grant of authorization with an export license (Department of State, 2015; United States Department of Commerce, 2015a; Department of Commerce, 2015b).

The DoD agency tasked with documenting the foreign collection threat to American industries also considers export control violations to be a type of espionage. To pursue its mission to "secure the nation's technological base," the Defense Security Service (DSS) oversees and monitors the thousands of contractor companies that have been granted facilities clearances by the federal government to handle classified or sensitive information. DSS collects reports from these cleared companies on attempts by foreign individuals or governments to acquire controlled information or technologies. DSS analyzes and compiles these reports in an annual publication that documents trends in foreign collection efforts in order to raise awareness and improve countermeasures. The 2014 version of this report, "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting," notes, "Cleared contractor reporting provides information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversion activities," and where warranted, DSS refers such reports to counterintelligence and law

enforcement authorities (United States Department of Defense, Defense Security Service, 2013).

DSS sponsors the Center for Development of Security Excellence (CDSE), a security education and training organization, which provides courses and certification for security personnel and the larger security community. One of CDSE's website pages, titled "Understanding Espionage and National Security Crimes," explains,

> U.S. defense information comprises more than just classified information. Targeting of defense information has included dual-use technology, military critical technology, sensitive company documents, proprietary information, and Export Administration Regulation (EAR) or International Traffic in Arms Regulation (ITAR) controlled technology. . . . ITAR and EAR are export control laws whose broad scope extends to products, software, technical details, and services, and includes both military and commercial items. (United States Department of Defense, Defense Security Service, Center for Development of Security Excellence, 2015)

The CDSE site goes on to explain, "along with traditional espionage and economic or trade secret espionage, ITAR and EAR violations must be reported to DSS by DOD security personnel for follow-up actions" (Department of Defense, Defense Security Service, Center for Development of Security Excellence, 2015).

Nine persons among the 209 individuals in this report violated export control laws because they transmitted restricted defense technologies or information. Table 20 lists them by cohort, and shows the information they compromised or attempted to compromise, their citizenship, level of clearance, and lists the countries that benefitted from their espionage.

**Table 20**
**Individuals Convicted of Export Control Violations**

| Name/Yr Began Espionage | Citizen-ship | Clearance | Recipient | Type of Information Passed |
|---|---|---|---|---|
| **Began 1947-1979** | **0 individuals** | | | |
| **Began 1980-1989** | **4 individuals** | | | |
| Ali, A. 1987 | natural-ized | none | Yemen | Night vision goggles, chemical weapons suits, body armor, classified documents |
| Hoffman, R. 1986 | native | TS | Japan | Software used to track missiles or rockets using exhaust plumes |
| Kota, S. 1985 | natural-ized | none | Soviet Union | Mercury cadmium telluride missile detectors, radar absorbing paint for stealth technology, biotechnology used to produce a synthetic hormone |
| Mak, C. 1983 | natural-ized | S | China | Electric-powered propulsion system, solid-state power switch for warships and submarines |
| **Began 1990-2015** | **5 individuals** | | | |
| Gowadia, N. 1999 | natural-ized | TS/SCI | China, Israel, Germany, Switzerland; attempted to Austria, Liechtenstein, 2 others unidentified | Exhaust systems for B-2 bomber, stealth avoidance using infrared sensors, radar-evading stealth exhaust nozzle for cruise missiles |
| Knapp, M. 2009 | native | none | Attempted to Iran, Russia | Anti-gravity flight suits, survival radios, F-14 fighter pilot ejection seats, F-5B Tiger II fighter jet airplane |
| Roth, J. 2004 | native | none | China | Plasma actuators for flight controls in automated weapons systems (drones) |
| Sherman, D. 2004 | native | none | China | Plasma actuators for flight controls in automated weapons systems (drones) |
| Shu, Q. 2003 | natural-ized | none | China | Cryogenic fueling system for space launch vehicles used in launch of satellites or space stations |

Eight of the nine individuals listed in Table 20 were convicted of violating, attempting, or conspiring to violate the AECA, the EAA, or the IEEPA. They also were convicted of additional charges, including: money laundering, income tax evasion, filing false tax returns, falsification, wire fraud, lying, and bribery of foreign officials. Two also were charged under AFGA, Amen Ali and Chi Mak. Noshir Gowadia was convicted of classic espionage as well as of export control violations, and Subrahmanyam Kota was initially charged with classic espionage but later had his charges reduced.

Kota had founded a software development company in Boston. Starting in 1985, he also developed a network of friends who worked in defense industries and were willing to collect information for him. Since he had no access himself, these friends provided sensitive or classified defense technologies, which he, in turn, sold to the Soviets. Specifically, Kota sold missile detection technology and stealth radar coatings for thousands of dollars.

Kota was caught in an FBI sting in 1994 while attempting to sell an international biotechnological breakthrough consisting of specialized cells from bioengineered hamster ovaries used to make an expensive drug that would stimulate human red blood cell production. In exchange for Kota's cooperation against an accomplice, prosecutors dropped the two espionage charges, and allowed him to plead guilty to selling stolen biotechnology and to income tax evasion.[58] While many of the technologies Kota compromised were clearly sensitive or classified and defense-related, he avoided prosecution on espionage and export control charges (Apodaca, 1995; Rakowsky, 1995).

The nine individuals listed in Table 20 were similar in some ways but not in others. Citizenship did not define them: four were native-born and five were naturalized citizens. Only three held clearances: Hoffman a TS, Mak a Secret, and Gowadia a TS-SCI at various stages of his career. Information and technologies can be designated "restricted" on the CCL or the USML and, thus, require an export license, yet not be classified. With dual-use technologies, a designation could depend on whether a commercial or military source was sponsoring and funding the research and development, as well as on the stage of the item's development when it was compromised.

Recipient countries for these nine persons included the usual suspects: China (recipient in five of the nine cases), the Soviet Union or Russia (two cases), and Iran (one case). However, other recipients were neutral or allied with the U.S., including Israel, Yemen, Japan, and various close allies of the U.S. that Gowadia approached.

Seven of the nine individuals were contractors to the federal government. Only Ali, who ran a cigarette store, and Knapp, who was unemployed after losing a job in human resources, were not. All seven contractors were scientists or other highly

[58] A jury later acquitted the accomplice, while the KGB agent whom the FBI had identified as the waiting buyer returned unhindered to the Soviet Union.

trained professionals: Hoffman was a rocket scientist and a physicist who worked on propulsion; Kota was a computer software engineer; Mak was an electrical engineer; Gowadia was an aeronautical design engineer; Roth, and his former student and protégé Sherman, were electrical engineers and plasma scientists; and Shu was an internationally recognized physicist working with cryogenics.

All nine individuals acted primarily for money. In addition, two were motivated by divided loyalties (Ali and Mak worked directly for the intelligence services of their foreign government sponsors), two were motivated by disgruntlement (Hoffman and Knapp), and four sought recognition and career advancement as well as money (Gowadia, Roth, Sherman, and Shu).

Knapp was discussed earlier as an example of someone who held no security clearance and attempted to transmit restricted but unclassified information and equipment. He also was an example of someone who was prosecuted for violating export control statutes. Working with an FBI undercover agent whom he thought was an arms broker, for 8 months in 2009 and 2010 Knapp procured restricted military hardware and tried to make money by selling it to Iran or Russia. Among other gear, he offered pilot ejector seats, emergency survival locator radios, anti-gravity flight suits, and an F-5B Tiger II fighter jet. He pled guilty to violating the IEEPA,[59] Executive Order 13222 that continues the EAA in force, and the AECA. He was sentenced to 46 months (3 years and 10 months) in prison (Department of Justice, 2011; United States Immigration and Customs Enforcement, 2011).

Gowadia committed both export control violations and classic espionage at the end of his aeronautical engineering career. Born in India, Gowadia came to the U.S. in the 1960s for postgraduate studies having already, he claimed, earned a Ph.D. at the age of 15. He began working for Northrop Corporation in 1968 and became a naturalized American citizen a few years later. Northrop was then developing the highly classified B-2 Spirit stealth bomber that combined various technologies to make it virtually undetectable to an adversary's radar and heat sensors. Gowadia focused on what became his area of specialization, the problem of hiding the infra-red signature from the B-2 bomber's jet propulsion. As the company merged to become Northrop Grumman, he continued on for 18 years and became the acknowledged expert on nozzle design until he left in 1986 (United States District Court for the District of Hawaii, 2007).

After retiring from Northrop Grumman, Gowadia founded his own consulting company to market his expertise in aeronautics and stealth design. His past experience allowed him to win contracts with DARPA and several other government agencies and military services, work a stint at Los Alamos National Laboratory in New Mexico, serve as an adjunct professor at three different universities, and

[59] IEEPA is at Title 50 U.S.C. § 1702 and 1705c; the E.O 13222 is at Title 31 C.F.R. § 560.204-560.205; the AECA is at Title 22 U.S.C. § 2778(b)(2) and § 2778(C), and Title 22 C.F.R. § 121.1, 123.1, and 127.1.

persistently seek and sometimes win international contacts (United States District Court for the District of Hawaii, 2007).

In the 1990s, Gowadia firmly established his international presence by setting up two overseas companies, one in Liechtenstein, a tax-friendly place from which to solicit contracts in Europe and to stash the earnings, and one in Canberra, which he opened with a former Australian Navy lieutenant commander. The Australian venture began when the Australian Defence Force (ADF) invited him to give a two-day seminar on stealth design. Pleased with his talk, officials encouraged Gowadia to set up a local company, and then paid him $1M (Australian) between 1999 and 2003 for services that included studies, training, and consulting on tests that applied his designs to the Australian C-130 transport plane. In 2003, however, negotiations over expanding Gowadia's work to other Australian aircraft failed after he demanded full ownership of any intellectual property (IP) that resulted from such a venture (McKenna, 2010).

In 1999, as he had begun to spend more time in Australia, Gowadia bought oceanfront land on Maui. In 2002, he finished building a lavish home there that sported a roofline shaped like a B-2. Months later, when the contract with the ADF collapsed, he faced a nearly $15,000 monthly mortgage on his new house without commanding some of the income he had expected would pay for it. As he had been doing for decades, he fell back on selling his expertise, but this time he focused on the Chinese (McKenna, 2010; Boylan, 2005).

His contacts with the Chinese began in January 2002 through a Chinese access agent named Henry Nyoo, which led to conversations with Tommy Wong, an official from the Chinese State Bureau of Foreign Exports. Wong and Nyoo worked the aeronautical research centers in the PRC to market Gowadia's offer to provide the Chinese with information and consulting services on how to develop their stealth capability for the Chinese air force. On July 29, 2003, Gowadia, Nyoo, and Wong flew to Hong Kong and then to Chengdu, the center of research and development in China for fighter aircraft and cruise missiles. Gowadia delivered a presentation on "low observable" propulsion systems, which included U.S. national defense information restricted from export and classified Secret (McKenna, 2010; United States District Court for the District of Hawaii, 2007).

Over the next 2 years, Gowadia made at least five more trips to the PRC. Between trips, he emailed classified data to the Chinese engineers he worked with, evaluated and corrected their test results, advised them on how to improve their testing and measurement facilities, oversaw the design of a nozzle for a cruise missile that would make it difficult to detect by radar, and provided the Chinese with classified flight test data that helped them modify their cruise missiles by showing them what "the exact 'lock on range' of a new Chinese missile would look like 'from a pursuing U.S. air-to-air missile'" (Gordon, 2005). According to Dean Wilkening, director of a science program at Stanford University's Center for International Security and Cooperation, "The reason foreign governments would like this [stealth] technology is

if they reverse engineer it, they can apply this to their fighter aircraft [and] if you do that, our air-to-air missiles don't work very well. They can't find the target" (United States Department of Justice, United States Attorney Edward H. Kubo, 2006; Gertz, 2006; Gordon, 2005).

Gowadia was arrested on October 26, 2005 after spending 10 days in voluntary interviews with the FBI. His house was searched, and many classified documents and reports were found (Macavoy, 2008). He signed statements admitting to having willfully conveyed national defense information to a person not entitled to receive it (Boylan & Perez, 2005; Dooley, 2009b).

After the first charge was filed, increasingly more serious indictments were handed down later in 2005, 2006, and again in 2007 as the investigations expanded around the world (United States Department of Justice District of Hawaii, 2010). While he remained in jail as a flight risk, his defense lawyers requested an evaluation for mental problems that could have made him incompetent to stand trial. The report on his psychological evaluation determined that he did suffer from a "narcissistic personality disorder," but a judge ruled in February 2010 that his grandiosity would not make him incompetent to stand trial, which began on April 13, 2010 (Sample, 2009; Associated Press, 2010).

Prosecutors announced during Gowadia's trial that the Chinese government had paid him $15,000 for his first trip, and later sent payments to his secret Swiss bank accounts that brought the total to $110,000. He had set up these accounts from Liechtenstein in the name of a fake charitable foundation for children.

While he was working for the Chinese in 2002 and 2004, he also had sent classified information to the Swiss government and to businessmen in Israel and Germany with marketing offers to apply stealth technology to various aircraft in those countries. In all, Gowadia made offers and disclosures to eight countries, including two countries not specified (United States District Court for the District of Hawaii, 2007; Department of Justice, 2011).

Although his defense attempted to prove that the information and services he had admittedly shared with the PRC had not been classified but were publicly available, Gowadia's initial confession was difficult to overcome in court (Dooley, 2010; "Accused spy sold nothing secret," 2010). He had signed a statement admitting he had

> disclosed classified information and material both verbally and in papers, computer presentations, letters, and other methods to individuals in foreign countries with the knowledge that information was classified. . . The reason I disclosed this classified information was to establish the technological credibility with the potential customers for future business. I wanted to help these countries to further their self aircraft systems. My personal gain would be business. (Gertz, 2006)

Gowadia was convicted on 14 counts, including: two counts of willfully communicating classified national defense information to the PRC with the intent that it be used to the advantage of the PRC or to the injury of the U.S.; three counts of willfully communicating classified national defense information to persons not entitled to receive it in the PRC and elsewhere; one count of illegally retaining defense systems information at his Maui residence; four counts of exporting technical data related to a defense article without an export license in violation of the AECA; one count of conspiracy to violate the AECA; one count of money laundering based on proceeds from the AECA violations; and two counts of filing false tax returns for the years 2001 and 2002. Testimony revealed that he had not paid any federal income tax in the years between 1997 and 2005, and although it was difficult to sort out the laundered money, his private consulting firm had earned at least $750,000 between 1999 and 2003 (Department of Justice, 2011; Boylan, 2005).

On January 24, 2011, Gowadia was sentenced to 384 months (32 years) in prison and was initially sent to the supermax penitentiary in Florence, Colorado. In that same month, the existence of a new Chengdu J-20 Chinese stealth fighter plane was announced to the public (Dsouza, 2012). At Gowadia's sentencing hearing the prosecutor, Assistant U.S. Attorney Ken Sorenson, said,

> This case was unique in that we litigated know-how, the very concept of exporting your knowledge base that you derive, in whole or in part, from your activities working in United States classified programs. If you can take that and go sell it or market yourself on an international stage in secrecy to other governments and not suffer criminal sanctions for it, then we're in trouble. (Niesse, 2010)

Gowadia was an example of someone who both illegally exported defense information and services and, at the same time, knowingly transmitted classified national defense information to a foreign government. Thus, he is coded as both a case of classic espionage and a case of export control violations. He also provides an example of someone who worked on important government technologies and sought to sell his expertise through espionage. "On reflection," he wrote in a statement written after his arrest, "what I did was wrong to help [the] PRC make a cruise missile. What I did was espionage and treason" (Dooley, 2009a).

Shu, on the other hand, was trying to help the Chinese and enrich himself in the process, but the information he transmitted was not classified national defense information. Rather, it was restricted from export by the export control laws. Between January 2003 and October 2007, Shu attempted to broker a three-way deal worth $4 million among the Beijing Special Engineering Design Research Institute (BSEDRI) in the PRC, an unnamed French company in Paris, and Shu's sole-proprietor company, AMAC International, Inc., in Newport News, Virginia. He did not realize, however, that for most of that time, he was being watched, tracked, and listened to by the FBI, U.S. Immigration and Customs Enforcement (ICE), and

DoC's Office of Export Enforcement (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Shu was born in Shanghai, attended college in Beijing, and earned a Ph.D. in physics in 1970 at the Institute of Low Temperature in Hangzhou, China. He launched his professional career in cryogenics (i.e., low temperature physics) in China, working at the Institute itself for 7 years, then becoming an Assistant Professor, and, in 1985, a full Professor of Physics at Zhejiang University in Hangzhou. Starting in 1983, he began to divide his time between his academic duties in Hangzhou and various research positions in the U.S., first at the University of Washington in Seattle, then at the Fermi National Accelerator Laboratory near Chicago. In 1998, Shu became a naturalized American citizen and in that same year, he incorporated his company in Virginia. AMAC competed for small business research grants to do specialized research in cryogenics for government agencies, including the Department of Energy (DOE) and the National Aeronautics and Space Administration (NASA). AMAC also maintained a second office in Beijing (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

One research grant allowed Shu to hone his company's expertise in the cryogenic transfer and storage technology of liquid propellants used in aerospace applications. AMAC developed an energy-efficient cryogenic transfer line with magnetic suspension for NASA's Kennedy Space Center that promised to extend space missions, save cryogenic fuel, and reduce overall launch mass. Projects like this enhanced AMAC's international reputation (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

As part of its extensive modernization effort, in the early 2000s the PRC began to plan its fourth and newest space launch facility on the island of Hainan. This would house heavy payload launch vehicles designed to send space stations and satellites into orbit. The facility also would provide support for manned space flight and future lunar missions. When Chinese astronauts walk on the moon, they will be launched from Hainan (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Such space vehicles use a combination of liquid hydrogen and liquid oxygen as their fuel, and these require very low temperatures to produce, store, and use. Shu offered to assist with China's systematic expansion of their space program at Hainan by providing his technical expertise in cryogenics and his knowledge of where and how to acquire foreign technology for cryogenic pumps, valves, transfer lines, and refrigeration equipment—all of the components that would be necessary to produce liquefied hydrogen and oxygen at the launch facility. Shu relied on emails and phone calls to court high-ranking BSEDRI officials and officers of the 101 Institute, which was tasked with implementing the project, from his offices in Beijing and Newport News. He also helped to arrange for PRC officials to visit various European space launch facilities and hydrogen production and storage

facilities so they could see the best examples for themselves (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).

Starting in January 2003, Shu began shuttling among the PRC, the AMAC office in Newport News, and Paris every few months. By August, he had Chinese approval to provide technical design work, and by November, he had entered the bidding on the project, proposing that AMAC would be the broker between the Chinese and the unnamed French company that would actually provide and test the equipment. He would provide the expertise in cryogenics along with the necessary Chinese language and cultural awareness skills. Through 2004 and 2005, Shu followed the evolving project and kept the French apprised of changes and new opportunities. Between December 2005 and January 2007, he actively negotiated a deal in which the PRC would buy liquid hydrogen tanks and associated equipment from the French company, and for its services, AMAC would receive a commission from the French. On January 15, 2007, the contract was finalized, and soon thereafter, Shu received the first two wire transfers from Paris totaling $253,962. Eventually he would receive $386,740 (United States Department of Justice, Federal Bureau of Investigation, "Redacted affidavit," 2008; United States Department of Justice Eastern District of Virginia, Press release, 2008).

The negotiations had been delicate. Shu directed his employees to make up the names of end-users for the export paperwork so as not to admit that the Chinese military was involved in light of the U.S. embargo on exporting such data and articles to the PRC. To one of his employees in Beijing, he explained that the Chinese would not be telling the French company everything, because the actual use for the product would "involve the military aspect," and this fact would not be released to outsiders. He also warned the French not to include too much detail in their specifications, lest the Chinese be able to reverse engineer the equipment and manufacture it for themselves, cutting AMAC and the French out of the deal.

Kickbacks were an expected part of the transaction. Shu offered three key PRC officials 3% of the estimated $4 million deal, but there was haggling. Chinese officials suggested that German and Russian bidders were offering 5%, while a senior Chinese official passed the word that he would require an additional 2%, along with Shu's assurances that no other Chinese officials would know about this addition—a suggestion having been passed along to Shu from the very Chinese officials who were not supposed to know about it (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008).[60]

As Shu was pulling these threads together into a deal, on July 21, 2006, two special agents from DoC's Office of Export Enforcement walked into the AMAC offices in Newport News and announced that they were there to give Shu an

[60] The FBI's "Redacted Affidavit of Criminal Complaint and Arrest Warrant for Shu Quan-Sheng" dated September 19, 2008, reproduces verbatim many of Shu's verbal interactions with his employees, the Chinese, and the French based on telephone and email monitoring. The affidavit is widely available online.

"outreach briefing." They explained to Shu that brokering an export deal between an embargoed country (China) and a foreign nation (France) counted as an American export. This briefing was to serve as a refresher on the export control regulations and also, one would assume, as a warning that the potential exporter was being watched. Shu responded by simply trying to be a more careful dissembler. He told an employee to make up end-users and uses entries on reports because

> if we said that was for launching satellites, we wouldn't be able to get that 101 [Institute] deal that's worth three million. . . Everyone hides it. . . . In the end, the manufacturers also help to hide it. The French, also. If you said you wanted to launch, eh, rockets or something, then France won't be able to sell to you. . . France belongs to NATO. . . . Let me tell you, that's how the military industry buys things. Right, we've done military industry business. (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008)

Shu was arrested on September 24, 2008, and charged with: unlawfully and willfully exporting a defense service to the PRC without a license; unlawfully and willfully exporting a defense article; and willfully bribing, offering a bribe, and attempting to bribe, a foreign government official (United States Department of Justice, Federal Bureau of Investigation, Redacted affidavit, 2008). After 2 months, he pled guilty to all three charges, and on April 2, 2009, he was sentenced to 51 months (4 years and 3 months) on each count, to be served concurrently. He also paid back some $387,000 in restitution to the federal government. "America has provided me with such a wonderful working environment and opportunity," Shu said at his sentencing hearing. "I would never deliberately harm the country I love" (Potter, 2008).

What Shu did was a type of espionage, and his offenses can be described in terms of the classic espionage categories that previously have been applied.

- A context of competition. The U.S. and the PRC are engaged in economic, military, and ideological competition for international advantage. Counterintelligence officials and China experts point to the Chinese as a growing threat, because they are one of the most effective and persistent collectors of American economic and technological information (Hannas, Mulvenon, & Puglisi, 2013).
- Secret means. Shu tailored the information he shared with each player in his deal, keeping some aspects secret from the others and warning them not to be too transparent with each other (United States Department of Justice, Federal Bureau of Investigation, "Redacted Affidavit," 2008).
- Goal is secrets. The data and the expertise Shu gave to the Chinese were not classified national defense information, but were restricted by the USML. In addition, the U.S. has had a trade embargo against the PRC since 1989 because

of the events at Tiananmen Square, making brokering any trade deal with the PRC another clandestine activity (McGlone, 2008b).

- Political, military, economic secrets. The data and expertise Shu offered related to essential elements of a technology needed to launch heavy payload space vehicles such as satellites, space stations, and rockets. The Chinese are developing their capabilities in space technologies, thereby challenging the U.S. supremacy in space, which has political, military, and economic implications for the American programs (United States Department of Justice, The Eastern District of Virginia, 2008).
- Theft. Shu is not reported to have committed theft in the course of his other crimes.
- Subterfuge. Shu repeatedly advised each of his two clients to withhold information from the other. He asked his employees in Beijing to use only fax to communicate with him because he did not want to let his American employees know all the details of his deals. He asked to communicate directly with Chinese officials rather than go through his employees in Beijing because he did not want them know all the details. He directed his employees to falsify export control forms with fake end-user names and uses for articles in order to evade export control regulations. When AMAC drafted a letter of invitation from the French company to officials at Institute 101, a military agency, to facilitate the PRC officials' visas to visit France, AMAC explained the Institute would not be named on the application because it was confidential. Instead, a fictitious company, China Great Wall Industry Corporation, would issue the invitation. In a phone conversation with an AMAC employee, Shu explained, "Everyone hides it [the military end use]" (United States Department of Justice, Federal Bureau of Investigation, Redacted Affidavit, 2008).
- Surveillance. Shu is not reported to have gathered information through surveillance, although he did engineer visits to similar space installations for his clients.
- Psychological toll. Shu appeared shocked when he was arrested and charged with export control violations. He seems to have regarded his activities as typical business dealings, and despite receiving explicit warnings in person, did not recognize that American authorities would see what he was doing as a crime. Observers reported that he appeared "shaking and bewildered" at his initial court appearance (McGlone, 2008a).
- Illegal. Shu was convicted of two counts of export control violations and one count of attempting and actually bribing foreign officials, sentenced to prison, and required to pay restitution (Potter, 2008).

## ECONOMIC ESPIONAGE

Given its name, it would seem obvious that economic espionage is indeed espionage. It may be necessary, however, to explain how economic espionage can be committed against the U.S. by American citizens. Economic espionage shares the basic categories and is intertwined with other types of espionage, yet there are unique elements that make it distinct from the four other types previously discussed.

The phrase "economic espionage" is often inexact. One may see it used interchangeably with "industrial" or "corporate" espionage. Most often, economic espionage refers to theft of information by or for a foreign government, a loss which could have implications for the whole economy of a nation, while "industrial" or "corporate" espionage typically refers to theft from one company by another. Although domestic, such thefts also may have far-reaching economic impacts.

### Trade Secrets

One of its unique elements is that the target of economic espionage is a trade secret and not, as in classic espionage, controlled government or military secrets about intentions, capabilities, plans, or technologies. Usually, the secrets in classic espionage are controlled by classification. A trade secret, on the other hand, is IP that was created by a business, which takes steps to keep it a secret, and from which the business derives value because it is not publicly known. A trade secret is not classified by the government, because the government does not own it.

There are several varieties of trade secrets, including:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public. (Economic Espionage Act, 1996)

Any enterprise can create, declare, value, and control its own trade secrets. A government agency does not determine its value or its legitimacy, as is the case with patents or licenses to export. So, why does the government get involved in

helping to secure the secrets of businesses, which typically have their own corporate security programs?

As democratic capitalism has evolved in the U.S., the government has assumed the role of the neutral arbiter to foster a fair and open marketplace, subject to the rule of law. To that end, it provides rules—through laws and regulation—for the conduct of business, and it provides sanctions for not following the rules (Heskett, 2009). Until 1996, the only choice for prosecuting unlawful misappropriation of trade secrets was under state laws, but because state laws varied, inconsistencies developed. Gradually, starting in the 1980s, all but four states adopted the UTSA, in which Congress provided a model law with uniform definitions and approaches that could apply across states, and these inconsistencies were reduced (United States House of Representatives, Committee on the Judiciary, "Trade Secrets" 1996). By the mid-1990s, however, as more and more IP came to be created and stored electronically, and as globalization knit together the world's markets, alarm over the increasing theft of trade secrets led Congress to consider the EEA of 1996, the first federal statute to address economic espionage.

The legislation acknowledged an emerging reality: the success of private enterprise in the U.S. was becoming so important to national security that the federal government needed to protect it. If competitors, especially foreign governments, could steal American trade secrets with impunity, the advantages for national security that economic strength conferred could be lost (United States House of Representatives, Committee on the Judiciary, "Trade Secrets" 1996). This is a second element of economic espionage that makes it unique among the various types of espionage: the federal government takes some responsibility for protecting secrets created and owned by private companies.

The United State House of Representatives Committee on the Judiciary debated the legislation that became the EEA. In its report to the House in September 1996, it recommended quick passage of the proposed law and explained in urgent terms the concerns that had prompted the Committee to act:

> As the nation moves into the high-technology, information age, the value of these intangible assets [i.e., trade secrets] will only continue to grow. Ironically, the very conditions that make this proprietary information so much more valuable make it easier to steal. Computer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.
>
> This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft. The information is pilfered by a variety of people and organizations for a variety of reasons. A great deal of the theft is

> committed by disgruntled individuals or employees who hope to harm their former companies or line their own pockets. In other instances, outsiders target a company, systematically infiltrate it, and then steal its vital information. More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies.
>
> The term economic or industrial espionage [the terms are used interchangeably here] is appropriate in these circumstances. Espionage is typically an organized effort by one country's government to obtain the vital national security secrets of another country. Typically, espionage has focused on military secrets. But as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind.
>
> It is important, however, to remember that the nature and purpose of industrial espionage are sharply different from those of classic political or military espionage. The phrase industrial espionage includes a variety of behavior—from the foreign government that uses its classic espionage apparatus to spy on a company [This concern would be addressed in Section 1831 of the Act], to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics [These concerns would be the focus of Section 1832 of the Act]. All of these forms of industrial espionage are problems. Each will be punished under this bill.

Other countries treat the relationship between their government and their economy differently, and this difference fuels some of the most aggressive economic espionage against the U.S. There is a spectrum across nations of how closely economies and governments are aligned. In the former Soviet Union and in the PRC, for example, the economy and the state were essentially the same. Both of these nations have moved away from their strict Communist policies to incorporate versions of capitalism, but they continue to operate under economic nationalism, in which the central party tries to control and direct the private enterprise that it does allow.

American allies also fall in various places along this spectrum. For example, the government controls over half of the industrial base in France, and it can be an assertive collector of economic intelligence. Such nations may gather intelligence from foreign companies to convey advantages to their own nation's companies, and they see this as a legitimate role for their governments (Lotriionte, 2015).

The U.S. government espouses a position at the other end of the spectrum, and emphasizes separation from and minimal interference with private enterprise. This

has led the U.S. to declare that it will not use the intelligence apparatus of the federal government to conduct economic espionage against other nations for the benefit of American companies. In 2013, then-Secretary of Defense Robert Gates reaffirmed this approach, saying that he refused to slide into what he called "the moral and legal swamp" of economic espionage (Lotrionte, 2015).[61]

### The Economic Espionage Act of 1996

The EEA was intended, in part, to protect American trade secrets from the ever more sophisticated theft of trade secrets by the intelligence-gathering operations of other nations (Foreign Press Center Briefing Transcript, Woolsey, 2000).[62] It criminalizes two related activities: economic espionage in Title 18 § 1831, and the theft of trade secrets in Title 18 § 1832. Section 1831, economic espionage, is the statute most directly relevant to this study since it implies foreign involvement, although in practice, the two sections are sometimes related to one another.[63] Section 1831 provides:

> (a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; [or]
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; [or]
> (3) receives, buys, or possesses a trade secret, knowing the same to

---

[61] Catherine Lotionte's comprehensive discussion of the relationship between classic and economic espionage considers the ways in which the U.S. collects economic intelligence against other countries (as opposed to engaging in economic espionage against them) and how it seeks to help American companies in activities such as trade negotiations. One of the vexing aspects cited by Gates of the government doing economic espionage on behalf of American companies would be deciding which companies to advantage. (See Catherine Lotionte, "Conquering state-sponsored cyber-economic espionage under international law," *North Carolina Journal of International Law*, 40(2), Winter 2015, 443-541.)

[62] James Woolsey's statement to the foreign press in 2000 gives the American position that the government does not engage in economic espionage, except in three instances: potential nuclear proliferation, monitoring sanctioned nations that hide their activities, and uncovering bribery that distorts competition unfairly. (See Foreign Press Center Briefing Transcript, "Intelligence gathering and democracies: The issue of economic and industrial espionage," briefing by James Woolsey, March 7, 2000.)

This paragraph only skates across the surface of the broad topics of economic and political change before and since the fall of the Soviet Union, and the impact of increasing globalization since then. It is intended only to mention some relevant topics as starting points for understanding the context of economic espionage. The discussion in Robert Gilpin with Jean Millis Gilpin, *The challenge of global capitalism*, Princeton, NJ: Princeton University Press, 2000, discusses that context.

[63] Here the elements in the federal law on economic espionage are taken as the definition and scope of economic espionage. Other authors, however, define the term economic espionage differently or more broadly.

> have been stolen or appropriated, obtained, or converted without authorization; [or]
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.
> (b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined the greater of $10,000,000 or three times the value of the trade secret to the organization. (Economic Espionage Act, as amended, 1996; White & Case Technology Newsflash, 2013)

The designation of a "foreign instrumentality" as one of the proscribed recipients of economic espionage, in addition to a foreign government or a foreign agent, is meant to cover entities directed by but not publicly linked to a foreign government. As defined in the EEA, a foreign instrumentality would include "any agency, bureau. . . component, institution, association, or any legal commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government (Economic Espionage Act, 1996; Reilly, 2009). For example, many foreign instrumentalities operate in the PRC under academic, research, corporate, military, and government auspices, which demonstrates the necessity of this language (Hannas, Mulvenon, and Puglisi, 2013).

Section 1832, on the other hand, deals with domestic trade secret theft. It resembles Section 1831 in that it criminalizes the misappropriation of trade secrets, but in 1832, there is no foreign government nexus required. Instead, 1832 deals with corporate or industrial espionage carried on between American companies. It is the theft of trade secrets from one company by another company or by employees of that company.[64] Section 1832 provides that:

> (a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

[64] A complication not addressed by the EEA in either of these two main sections is the American company which maintains offices overseas. Unless an overseas theft was committed by an American citizen, it is not protected under the EEA (Simon, 1998).

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
>
> (b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000. (Economic Espionage Act, 1996)

While the two sections share a focus on protecting trade secrets, they differ in several important ways. One difference is in how they specify the perpetrator's intent. Section 1831 requires only that a person "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly steals", while Section 1832 requires two different intentions. First, a person must have an "intent to convert a trade secret. . . to the economic benefit of anyone other than the owner thereof," and second, a person must be "intending or knowing that the offense will injure any owner of that trade secret." The thief may be, but does not have to be, the one who benefits from the theft, and while the beneficiary does not need to be a foreign government as in 1831, in 1832 the beneficiary could be a foreign government (e.g., one to whom an American thief planned to convey a stolen secret as a part of expatriating to that country, even if that country's government had not initiated the theft) ("Spotlight on the Economic Espionage Act," 2012).

A second difference between Sections 1831 and 1832 is how the potential benefit is specified. According to the House Judiciary Committee, in Section 1831 the benefit to a foreign government should be broadly framed. It "means not only economic benefit but also reputational, strategic, or tactical benefit" (United States House of Representatives Committee on the Judiciary, "Report," 1996). In Section 1832, however, the benefit is specifically economic.

A third difference is that because the emphasis in Section 1832 is on domestic crimes, in order to come under federal jurisdiction it must be about interstate commerce. Therefore, Section 1832 specifies that the trade secret must be "related to or a product or service used in or intended for use in interstate or foreign commerce" ("Spotlight on the Economic Espionage Act," 2012; Simon, 1998).

A potential confusion lurks because a person convicted of offenses under Section 1832 is accurately said to be convicted under the EEA, yet it is actually only Section 1831, with its foreign nexus requirement, that a crime is labeled "foreign economic espionage." Section 1832, as described earlier, punishes the theft of trade secrets. It would have been clearer if Congress had named its law "Economic Espionage and the Theft of Trade Secrets," which, while closely related, are not both economic espionage in terms of the EEA.

Since 1996, federal authorities have investigated and prosecuted cases under the EEA. By 2009, over 100 cases of trade secret misappropriation (Section 1832) had been prosecuted, in comparison with six cases of economic espionage (Section 1831) (Krotoski, 2009). As a guide for his fellow prosecutors, one federal prosecutor listed some common case scenarios that had emerged by that time, including the following:

- State-sponsored targeting of trade secrets and technology misappropriated with the intent to benefit a foreign government or an instrumentality of a foreign government.
- A trusted employee with access to valuable company information who, after becoming disgruntled, downloads and transmits the information to others outside the company who offer it to the highest bidder.
- An employee, who after learning how a new prototype is made, decides to form his own company and use the trade secret and other proprietary information to launch his own competing product.
- A competitor who devises a scheme to gain access to company information for use in fulfilling an international contract.
- Employees who execute a plan to steal proprietary information and take it to another country, but are stopped at the airport.
- After being offered a senior position with a direct competitor, and before tendering his resignation, an employee uses his supervisory position to request and obtain proprietary information he would not normally be entitled to access. After taking as much proprietary information as he can, he submits his resignation and takes the materials of his former employer to his new position and employer. (Krotoski, 2009)

One can discern in these scenarios the legal task of sorting out which section of the EEA would best apply, economic espionage or theft of trade secrets. While it may depend on the evidence that is available, one legal authority suggests that deciding whether what a company claims to be a trade secret is actually a trade secret may

be a job for the jury. He explains, "among the factors in assessing whether certain subject matter is a trade secret are the:

- extent to which the information is known outside of the company;
- extent to which it is known by employees and others involved in the company;
- extent of measures taken by the company to guard the secrecy of the information;
- value of the information to the company and to its competitors;
- amount of effort or money expended by the company in developing the information; and
- ease or difficulty with which the information could be properly acquired or duplicated by others." (Restatement (Third) of Unfair Competition § 40 (1994), quoted in Thomas, 2014)

Sometimes investigators of trade secret theft have the luxury of investigating an ongoing crime, developing their case by running an undercover agent, and collecting evidence over a period of time before arresting the suspect. Often, however, such cases are recognized as a theft at the last minute, and law enforcement must scramble to reach the airport in time to prevent the thief from getting on a plane for a foreign conference or a foreign country. Although a trade secret has no expiration time limit, once it is made public, its status as a trade secret is gone and cannot be recovered (Krotoski, 2009).

The paucity of economic espionage cases prosecuted since 1996, despite the urgency Congress expressed then and subsequently about how the draining away of American innovations needs to be staunched, has prompted critics to argue that the economic espionage section of the EEA needs to be redrafted. Critics of the EEA argue that based on the debates held during consideration of the legislation, the courts have so far interpreted Section 1831 more narrowly than Congress intended. This has made convictions harder to get, which, in turn, has discouraged DoJ from bringing more cases (Kuntz, 2013).

Others explain the small number of cases differently. Economic espionage cases are especially complex, and DoJ chooses to focus its resources on cases it is most likely to win, which is rarely true with EEA cases. Also, there are potential diplomatic repercussions in economic espionage cases that make prosecutors cautious. Finally, even though the EEA authorizes the court to issue protective orders to prevent a trade secret from being revealed during a trial, plaintiffs are still leery of a public trial where, with one slip of the tongue, their secrets could be lost (Thomas, 2014; Doyle, 2014; "Recent cases," 2012). Starting in 2010, however, DoJ shifted its priorities and has started prosecuting more economic espionage cases, and the FBI recently created an Economic Espionage Unit in its Counterintelligence Section (Coleman, 2014).

The increasing attention paid by federal authorities to protecting trade secrets reflects the ongoing evolution of the U.S. from its manufacturing base to a

knowledge- and service-based economy. This shift already was recognized in 1996 and could be seen in the Congressional debate on the EEA quoted earlier. Efforts by the government, and by American companies themselves, to keep control over IP, innovations, investments in new processes, creative insights, and "intangible assets" are not just advisable; control is essential to stay in business. One author notes, "In 1975, 16.8% of the total value of the S&P 500 reportedly consisted of intangible assets. In 2005, intangible assets reportedly constituted 79.7% of the total value of these firms" (Thomas, 2014).

Economic espionage conducted by and benefitting foreign countries is not just about whether particular companies succeed or fail; it is about how the nation fares overall. When other nations steal American trade secrets to advantage their own domestic companies, they disadvantage American companies and the U.S. itself. A student of espionage explains,

> IP theft results in the loss of revenue for those who made the invention as well as the jobs associated with those losses. It also undermines the means and the incentive to innovate, slowing the development of new inventions and industries that would otherwise expand the economy and raise the prosperity and quality of life for everyone. The negative impact from IP theft on core values is global and staggering. (Lotrionte, 2015)

Since 1996, when Congress thought in terms of spies pocketing diskettes, our widespread reliance on enhanced technologies has only grown, and the ease of capture, storage, and movement of data has made controlling valuable intangible assets more difficult. Thus, discussions of economic espionage usually raise two additional topics: cyber espionage (discussed further), and insider threats (discussed in an essay in Appendix A) (Thomas, 2014; Office of the National Counterintelligence Executive, 2011; "Economic impact of trade secret theft," 2014).

Various outcomes have been reached for the 10 cases prosecuted under Section 1831 between 1996 and 2015, some of which have involved multiple defendants. In six cases, defendants were convicted of economic espionage under Section 1831. In two other cases, individuals who had been charged under Section 1831 were acquitted of that charge, but convicted of the related Section 1832 offenses. One case led to an acquittal, and in several others, the defendants fled. At least five of the principal defendants were American citizens,[65] and of those, four were convicted under Section 1831. One of these, Walter Liew, was sentenced in July 2014, too late to be included in the data for this study. Two others, Fei Ye (who pled guilty in

[65] It can be difficult to ascertain citizenship from summaries available in open sources, perhaps because economic espionage cases do not attract the attention of the press to the same degree that classic espionage cases do. An otherwise excellent compilation of case summaries published periodically by the Department of Justice, National Security Division, titled "Summary of major U.S. export enforcement, economic espionage, trade secret and embargo-related criminal cases," the latest of which is dated August 2015, does not consistently report citizenship.

2006) and Elliott Doxer (who pled guilty in 2011), were not included in this study but will be considered for inclusion in the future.[66] The only individual convicted of economic espionage who is included in this study is Dongfan (Greg) Chung, who spied for the Chinese for at least 25 years (Krotoski & Harrison, 2015).

Chung was born in China in 1936, and immigrated with his family to Taiwan as the Chinese Communists came to power after World War II. He married in China, moved to the U.S. with his wife for graduate school, and became a naturalized American citizen in 1972. He worked for a series of defense contractors, including McDonnell Douglas, Rockwell, and Boeing. Starting in the 1960s, he served as a structural engineer on various defense projects, and eventually focused on the NASA space shuttle. For most of his later career, he did stress analysis on the shuttle's forward fuselage section, and held a Secret security clearance. In 2002, the Boeing facility where he was working relocated, and Chung retired rather than move from Orange, California, where he and his wife had built a house. The next year, however, at age 70, he was rehired by Boeing as a subcontractor to help with the analysis of the Columbia shuttle crash (United States District Court Central District of California, Indictment, 2008; Bhattacharjee, 2014).

After Mao Zedong's death in 1976, China began rapidly modernizing and its economy began to accelerate. The Chungs were active in a Taiwanese immigrant association, but they began to feel constrained by the strident nationalism the group expected toward Taiwan. They wanted to understand what they had missed out on because their families had left China when they were young. During the late 1970s, it became possible to meet visiting Chinese scientists at conferences in the U.S., and Chung made such contacts. The Chinese government encouraged Chinese visitors to gather any technological knowledge they could from the West (Bhattacharjee, 2014).

In 1979, Chung met a visitor from the Harbin Institute of Technology. When the visitor expressed interest in problems of stress analysis, Chung sent copies of his graduate course notes on stress analysis via sea freight. In a letter to this contact, found later during the investigation, Chung wrote, "I don't know what I can do for the country. Being proud of the achievements by the people's efforts in the Motherland, I am regretful for not contributing anything" (Bhattacharjee, 2014).

---

[66] Fei Ye, a naturalized American citizen, along with an accomplice who was a Chinese national, pled guilty to two counts of economic espionage and one count of possessing stolen trade secrets dealing with the design and manufacturing of computer microprocessors in December 2006. They admitted they intended to use the trade secrets in a company they were setting up in the PRC, a project that was sponsored and funded by provincial Chinese authorities in the region where their company would be located. Elliott Doxer, a Jewish American citizen, sent an email to the Israeli consulate in Boston in June 2006 offering to help Israel by passing along his employer's trade secrets. Doxer worked for Akamai Technologies, which delivered content over the Internet handling between 15% and 30% of global internet traffic. In an FBI undercover sting, Doxer passed along to the agent, who he thought was an Israeli, Akamai's contractual papers, customer lists, and employee lists. In August 2011, Doxer pled guilty to one count of economic espionage. Both Fei Ye and Doxer received sentences of 1 year (Krotoski & Harrison, 2015).

Opportunities to contribute to China's achievements were regularly presented to Chung in a coordinated Chinese intelligence gathering operation starting in the 1980s, and continuing until 2003. He received invitations to meet with Chinese officials at gatherings in California, and in 1985, he was asked to visit China to lecture on his expertise in aerospace, one of the areas China had identified as critical to its technological advancement.

After the Chung family's visit to China in 1985, which lasted for several months, he came home with eight pages of questions from engineers at the Nanchang Aircraft Manufacturing Company. He pulled together his answers and sent along 27 volumes of engineering manuals for the design of the B-1 Bomber via diplomatic pouch from the Chinese consulate in San Francisco. For the next 20 years, Chung brought around 300,000 pages home from Boeing Corporation to save for or to send to the Chinese ("Ex-Boeing engineer, 2009; Flaccus, 2010).

Chung came to the attention of the FBI in the same way that Kuo did: Chi Mak, had written their names and their contact information in his own address books, which the FBI found in October 2005 when they surreptitiously searched his home. For at least a decade, Mak had served as the local handler for both Kuo and Chung, sending taskings from China and collecting information to send back. A second search yielded a letter between Chung and Gu Weihao that Mak had kept. Gu was a Chinese official with the China Aviation Industry Corporation, and he asked Chung for information about airplanes and the space shuttle, and thanked him for technical information he had previously sent.

The FBI arrested Chung on February 11, 2008 after several interviews, secret searches of his trash, and a search of his home which revealed the thousands of Boeing documents stockpiled in basement rooms and crawl spaces. The indictment outlined evidence of his regular interactions with Chinese officials: their discussion with Chung of cover stories for his visits to China; the advisability of sending information through Mak because it was "faster and safer"; Chung's repeated and earnest expressions of his desire to help China; his technical responses to their questions and requests; his removal from Boeing of books, reports, and hundreds of documents; and his travel to present lectures in China which he failed to report to Boeing security managers in spite of reporting requirements (United States District Court Central District of California, Indictment, 2008).

Prosecution moved slowly despite the volume and nature of the information Chung removed from Boeing facilities, including 2 decades' worth of trade secrets on the space shuttle, specifications on a fueling system for the Delta IV booster rocket, and the technical details on the C-17 military transport aircraft. Although the materials were proprietary and had been developed for the federal government, they were not designated as national defense information and were not marked as classified (Flaccus, 2009, United States Court of Appeals for the Ninth Circuit,

2011).[67] Thus, prosecutors shifted from their intention to charge Chung with espionage and instead charged him with economic espionage. To prove that the Boeing information included trade secrets, they presented testimony from Chung's Boeing colleagues about the restricted and export-controlled nature of the information, the proprietary agreements employees signed, and the nondisclosure agreements everyone signed to obtain a Secret security clearance and have access to such information.

Chung requested a bench trial and became the first person convicted at trial under the EEA (Flaccus, 2009). He was convicted in July 2009 of six counts of economic espionage, one count of lying to the FBI, one count of acting as an agent of a foreign power, and one count of entering into a conspiracy with Mak (Ex-Boeing engineer, 2009). He was sentenced on February 8, 2010, to 188 months in prison (15 years and 7 months) for betraying information that had been developed by Boeing over 5 years at a cost estimated to have been at least $50 million (Flaccus, 2010).

Economic espionage is a distinct type of espionage, one that is similar to classic espionage in many respects, but different in others. Applying the characteristics of classic espionage discussed in the chapter earlier to this economic variant demonstrates this.

- A context of competition. The competition for Chung was less that between the defense contracting companies he worked for, and more the international competition between the PRC and the U.S.
- Secret means. Chung conspired with his handler to secretly pass information to the PRC. Chung's contacts in China developed cover stories he could use to explain why he and his family were spending 2 months traveling in China in 1985. As the FBI was starting to explore Chung's involvement with China, they repeatedly searched his trash and each time, they found Boeing proprietary documents interleaved into Chinese language newspapers in attempts to secretly dispose of them (United States District Court Central district of California, Southern Division, "Memorandum," 2009. This "Memorandum of Decision" written by the judge in Chung's trial is the source for the remaining entries in this list, unless otherwise noted.)
- Goal is secrets. The goal in economic espionage is trade secrets. The FBI found detailed task lists from the Chinese in Chung's home that specified the information they most wanted. Included on these lists were: aircraft design manuals; fatigue design manuals; materials manuals; S-N curve manuals; military specifications user manuals; fighter jet structural details design

[67] At various periods of time, information was designated as restricted from export, proprietary to the companies working on defense contracts, and eventually could have been classified. Work on elements of technology within a large government program proceeds in stages, however, and the type and degree of control over information varies. One student of espionage noted, "The Chinese. . . are good at positioning agents who can obtain advanced technology in the developmental stage, before it is classified" (United States District Court Central district of California, Southern Division, "Memorandum," 2009; Gertz, 2006).

manuals; space shuttle design manuals; information on the shuttle's environmental conditions, airtight cabin, heat resistant tile design, and materials composition process; the life-span extension/reliability analysis of U.S. fighter planes and airborne equipment; and S-N curves for fighter plane cabin Plexiglas and cabin canopies. The intense interest in what Chung could provide about space technologies reflects efforts by the PRC to catch up as quickly as possible by using technologies already designed by others (Elmhirst, 2009).

- Political, military, economic secrets. The information Chung stole from Boeing and sent to the PRC related to U.S. space and military technologies. As Boeing's trade secrets, they were economic, but because Boeing is a defense contractor, many of them also were restricted military information.
- Theft. Chung exfiltrated over 300,000 pages of Boeing documents, manuals, and reports over the years he worked for the company.
- Subterfuge. Chung stored these stolen documents all over his house, some in hidden places, but others in plain sight. These storage places included the crawl spaces and a specially-constructed camouflaged storeroom hidden under the house, as well as under the stairs, in the fireplace, in stacks on tables in the dining room, and under the bed. In his exchanges with his Chinese contacts, Chung demonstrated his awareness that what he was doing required subterfuge (e.g., using a secure channel provided by his handler, and traveling to China under the guise of a family vacation to meetings where he could present information "in a small setting, which is very safe").
- Surveillance. Chung sought out opportunities at Boeing and in the course of his work interacting with other companies to collect specific information requested by his Chinese contacts.
- Acted as an Agent of a Foreign Government. In his close and ongoing relationships with contacts in the PRC and in the Chinese consulates in California, Chung took direction and acted in their interests. He was convicted of one count of Acting as an Agent of a Foreign Power, Title 18 U.S.C. § 1951.
- Psychological toll. During his long espionage career, Chung is described as serene in his workplace and personal life. He wrote to his contacts expressing his pleasure to be contributing to the modernization of China. When the FBI came to interview him, search his home, and arrest him, Chung was noticeably rattled, as if surprised at this response to his activities.
- Illegal. Chung was convicted of six counts of economic espionage: possessing trade secrets for the benefit of China (Title 18 U.S.C. § 1831); one count of lying to the FBI (Title 18 U.S.C. § 1001); one count of acting as an agent of a foreign government (Title 18 U.S.C. § 951); and one count of entering into a conspiracy with Mak (Title 18 U.S.C. § 371).

Like the other types already discussed, economic espionage can be described in the general terms of the model of espionage derived from classic espionage.

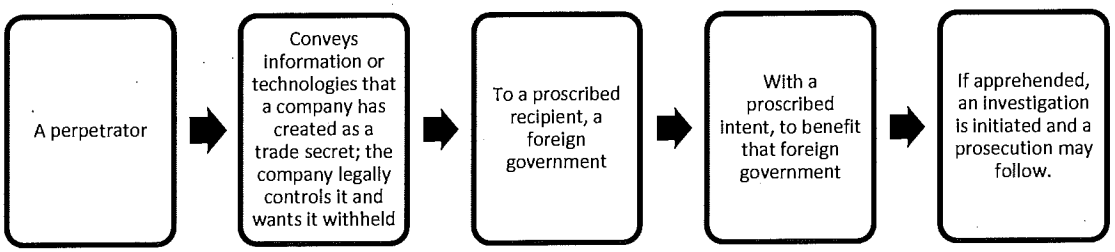



**Figure 7 Economic Espionage in a Model of Elements of Espionage**

In Figure 7, an individual who commits economic espionage conveys a trade secret to an agent of or a foreign government itself with the proscribed intent to benefit that government, thereby disadvantaging the company that owns the secret and the U.S. itself.

# PART 3

# CONTEXT AND RECOMMENDATIONS

## CHANGES IN CONTEXT THAT SHAPE CURRENT ESPIONAGE

Sweeping changes in context are shaping how espionage is conducted now and how it will be conducted in the future. Two of these changes that should be considered in any analysis of espionage are information and communications technology (ICT) and globalization. Examples discussed thus far have illustrated how recent spies have incorporated ICT advances into their activities, and how the worldwide market for American technologies has spurred the theft of export controlled and trade secret information.

### Information and Communications Technology (ICT)

During the past 2 decades, information technology (IT) and networked communications have become so ubiquitous that it can be difficult to step back and recognize some of the national security implications of what has become the new normal. Setting the scene for this context are statements from several officials, security professionals, and observers:

- The ubiquitous digitalization of information and pervasive connectivity of electronic networks have facilitated espionage as well as productivity. *Joel Brenner, former National Counterintelligence Executive and former Inspector General of the National Security Agency (NSA)* (Brenner, 2014)
- According to the Federal Bureau of Investigation (FBI), the theft of intellectual property (IP)—products of human intelligence and creativity—is a growing threat which is heightened by the rise of the use of digital technologies.[68] The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. *Gregory C. Wilshusen, Director Information Security Issues, Government Accountability Organization (GAO)* (Wilshusen, 2012)
- Can the government still keep a secret? In an age of WikiLeaks, flash drives and instant Web postings, leaks have begun to seem unstoppable. . . . Still, there's been a change. Traditional watchdog journalism, which has long accepted leaked information in dribs and drabs, has been joined by a new counterculture of information vigilantism that now promises disclosures by the terabyte. A bureaucrat can hide a library's worth of documents on a key fob, and scatter them over the Internet to a dozen countries during a cigarette break. *Scott Shane, reporter for the New York Times.* (Shane, 2010)
- Cybercrime and cyber espionage, both political and economic. . . are here and will remain the biggest cyber risks in the future. *Myriam Dunn Cavelty, Center for Security Studies, Swiss Federal Institute of Technology.* (Cavelty, 2012)

---

[68] Footnote in original is omitted here.

- Those conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis. *James R. Clapper, Director of National Intelligence* (Clapper, 2015)

In this report, various characteristics of espionage by Americans have been explored, along with the various types of espionage they undertake. This chapter briefly considers the impact of what the expert observers quoted above describe as ubiquitous, pervasive, and unstoppable trends in ICT that have revolutionized the way we communicate and conduct business.

The activities of cyber criminals[69] vary widely in scope, ranging from a lone hacker who opportunistically steals or sells another individual's personal information, to a foreign government that systematically attacks its adversaries' networks to disrupt critical infrastructures, take control of financial systems, overwhelm network functioning, and/or attack IT assets used for decision-making by military or government leaders. Two dimensions of this spectrum of cyber activities are relevant for understanding espionage by Americans: how an agent currently gathers, stores, and transmits intelligence to a foreign government; and how a foreign government steals controlled information directly across interconnected networks, usually in unacknowledged ways, with or without the help of an agent.

Reliance on computers began to spread from select military and academic users into the general population during the 1980s. IT became increasingly common during the 1990s, and after 2000, it was essential in business and professional settings. As these technical improvements became available, American spies adopted them to the extent permitted by their own technical proclivities and opportunities for use. Table 21 summarizes the increasing use of ICT among the 209 Americans in this study by decade.[70]

---

[69] The prefix "cyber" was first used in 1991, according to the Merriam-Webster dictionary. It is defined as "of, relating to, or involving computers or computer networks, i.e., the Internet." Thus, terms such as "cyberspace" refer to the virtual environment in which computers operate over networks. Cyber criminals are persons who commit crimes using computers across networks. Cyberespionage, as defined in a 2015 Congressional Research Service report, is committed by cyberspies, "individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. Targets include government networks, cleared defense contractors, and private companies" (Theohary & Rollins, 2015).

[70] Use of ICT by American espionage offenders was coded from open source descriptions that did not reliably mention these details, so these figures can only provide an impression of increasing use over time.

**Table 21**
**Use of Information and Communications Technology by Decade Espionage Began**

| Decade Espionage Began | Number Who Began Espionage in Each Decade | Number of ICT Users Coded[71] | % of ICT Users by Decade |
|---|---|---|---|
| 1970-1979 | 30 | 4 | 13 |
| 1980-1989 | 72 | 11 | 15 |
| 1990-1999 | 28 | 10 | 36 |
| 2000-2009 | 32 | 21 | 66 |
| 2010-2015 | 7 | 6 | 86 |

With the accelerating pace of technological innovation, the time lag has rapidly shrunk between when citizens of one country make a technological advance and when the rest of the world learns about and adopts it, and there is now a global technological race to keep up with the latest innovations as they appear (Limbago, 2014). Spies have moved with the times, from the paper documents, microfiche strips, and film canisters to floppy disks, CDs, flash drives, and encrypted email attachments.

### *Advantages and Disadvantages of ICT for Spies*

ICT innovations offer both advantages and disadvantages to espionage agents. Its advantages are apparent to anyone who owns a computer and accesses the Internet. For instance, spies can install software to quickly copy large electronic files or download files from network servers onto USB drives that are inconspicuous to carry and store. Such software also can exfiltrate information directly to unauthorized recipients. Spies can email encrypted information to a recipient anywhere in the world, thereby eliminating the risks associated with in-person meetings and dead drops that might be monitored by authorities ("Electronic spycraft," 2015). Among those individuals coded in the PERSEREC Espionage Database since 2000, 20 of the 27 known ICT users copied information from computers or downloaded it from networks. Twelve are reported to have sent information by email attachment, two by fax, and the rest on CDs inside old-fashioned postal mail or in shipping containers.

None of the 209 Americans included in this report possessed sophisticated ICT skills, but such a person is hardly unlikely to be operating as a spy in the near future. For example, Charles Eccleston pled guilty on February 2, 2016 to attempted unauthorized access and intentional damage to a protected computer

[71] A person's use of ICT may have occurred late in a long espionage career rather than in the decade in which the spy first began espionage. For example, Walter Kendall Myers and his wife Gwendolyn began spying for Cuba in the 1970s, but only relied on ICT as networked computers and email became common later in the 1990s.

system.[72] Eccleston sought revenge and money after the Nuclear Regulatory Commission laid him off, and proposed a spear-phishing idea to a foreign embassy, speculated to have been the Chinese. He schemed to collect email addresses and send electronic conference invitations to federal employees in nuclear laboratories that included a registration link that, when clicked, would plant a virus, damage the government computer systems, and enable exfiltration of classified nuclear-related information. Eccleston, however, was working with undercover FBI agents, so no damage was done (Department of Justice, 2016; Hsu, 2016; United States District Court for the District of Columbia, Indictment, 2015).

An agent like Eccleston who tries to leverage ICT to capitalize on employees' access can infiltrate computers or networks remotely, which adds another layer to the advantages ICT offers to espionage. With the right expertise, hacking into a target's computer or network can be an inexpensive way to collect information. It also offers the advantage of anonymity, since it is difficult to identify with certainty who was responsible for an intrusion (Schneier, 2015).

With even more determination, an agent can hack into a computer system and install malicious software that takes over a network and removes data, silently sending the desired information from the target's network to a destination designated by the agent (Schneier, 2015). Other means useful for espionage that are now available also include software focused on end-point vulnerabilities, such as keyboards and computer screens, which allow what is written or searched to be collected at the point of the target's keystrokes, often evading the best encryption. It also is possible to intercept wireless network signals and read what is sent in real-time by a target or potential asset ("Electronic spycraft," 2015).

In addition to its advantages, ICT tools also come with disadvantages. One observer notes, "A much bigger worry for spies is that the very vulnerabilities which make it easy for them to steal other people's secrets also make it hard for them to hold on to their own" ("Electronic spycraft," 2015). For example, cell phones generate metadata that can be traced to show the location of the user at a particular time, thus potentially placing a person at the scene of an information pick-up or a meeting. The times at which a cell phone user makes calls and to whom can be analyzed, which indicates when the person is awake and active, and thereby, signifies the person's approximate time zone. If an agency can track a person's movements, it becomes difficult to clandestinely meet assets or conduct surveillance. Cell phones also can be used as bugging devices, potentially allowing the authorities to listen in on conversations (Murphy, 2015; "Electronic spycraft," 2015).

As an example of ICT's double-edged sword, recall the investigation of Stephen Kim, the nuclear proliferation expert and contractor for the Department of State (DoS),

[72] Charles Eccleston will be sentenced later in 2016. He is not included in the 209 individuals in this study since his crime was revealed after the cut-off date for analyses, but he is discussed here as a timely example of a direction spies who are sophisticated with ICT are likely to take.

and James Rosen, a Fox News reporter. Kim and Rosen temporarily worked in the same DoS building, and they used their email accounts and cell phones to set up times and places to meet. FBI investigators were able to cross-reference badging records with electronic communication data to reconstruct a timeline of their plans, contacts, meetings, and shared files that led to Kim's conviction (United States District Court for the District of Columbia, Affidavit, 2010).

Some American espionage offenders entered the U.S. with the intention of building a career that would give them access to classified information they could send back to foreign governments. Larry Wu-tai Chin, Karl Koecher, and Chi Mak, all discussed earlier, are three examples of spies who came to this country as sleeper agents. Each left their previous lives at the border and either assumed new identities or shaded inconvenient elements of their pasts. This subterfuge may be more difficult now that biometric scanners are used at international airports and many offices and government buildings. These scanners record a person's biometric characteristics, such as fingerprints, iris scans, and facial patterns, and the electronic records of these scans can be kept indefinitely. This makes changing one's identity or assuming an identity in which some parts have changed—as Chin, Koecher, and Mak did—more difficult than it once was. Some speculate that in the future, spies may have to become "single-use operatives" who only can operate in the one country that has their biometrics, unless they operate in nations that do not share information. Even then, however, the spy could be compromised if someone in one of those nations sold sensitive biometric data to an adversary (Murphy, 2015).

Like biometric data, social media data could compromise a person's espionage career. The photos and personal news that people post persist on the Internet indefinitely, and this trail of personal data can haunt espionage agents just as it does anyone who tries to change careers or take a new direction in life. If a foreign agent uses social media, and then seeks an insider position in a government agency to gain access to classified information, posted photos are available to be compared against, again making it difficult to assume a new identity or a covert role. Of course, if a young person has no online social media presence, potential employers may infer that this person is trying to hide or cover something up, but suddenly discontinuing an established social media presence by "going dark" can be equally suspicious (Murphy, 2015). In short, social media offers agents valuable recruitment opportunities, but it also may tie them to specific identities.

### *Cyber Espionage by Governments*

The second dimension of the evolution of cyber activities to be considered here is how a foreign government now can steal controlled information directly across interconnected networks, with or often without the cooperation of an agent. The focus of this report is on the activities of American agents who work against the interests of the U.S., rather than on the activities of the foreign governments

themselves, but because this dimension of the cyber context is developing rapidly in scope and sophistication, it may soon change the role of espionage agent.

Before the spread of the Internet, governments typically spied directly on one another either by observation or by intercepting various signals the adversary emitted. Governments still use those methods, but new cyber methods offer relatively cheap, easy, and anonymous entry into the networks where a target's information usually resides, rather than in the safes or locked drawers used in previous decades. Observers report that over 30 governments around the world already have formed cyberwarfare divisions within their militaries to develop the means to infiltrate computers remotely and steal information (Schneier, 2015; Limbago, 2014).

Cyber intelligence—collecting, analyzing, and disseminating intelligence on the intentions, capabilities, and operational activities of foreign cyber actors—is one of the core objectives in the National Intelligence Strategy that the Office of the Director of National Intelligence (ODNI) produced last year to guide the activities of the Intelligence Community (Clapper, 2015). Since 2010, government agencies including the Department of Defense (DoD), Department of Justice (DoJ), Central Intelligence Agency (CIA), National Security Agency (NSA), Department of Homeland Security (DHS), and ODNI have reorganized to include cyber capabilities to gather intelligence, counter digital impacts, and, if necessary, conduct cyber offense (Viswanatha, 2014; Elkus, 2015; Bennet, 2015; 'New intelligence agency," 2014; Clark, 2015).

Cyber offense takes the form of illegally hacking into a target government's or military's networks to learn the network structures and explore the information contained therein, and then perhaps planting malware to silently extract data for days or months, taking the information directly and electronically that spies on the ground would have to maneuver and plot to obtain. Once inside a network, cyber offense can plant false information to mislead or disrupt the target, or it could even insert destructive malware, which on a remote signal from the intruders can damage the network or bring it down, denying the target its information and its coordination capabilities (Schneier, 2015; Office of the National Counterintelligence Executive, 2011).

These scenarios are not the stuff of movie plots or projections far into the future. All major world powers with advanced ICT systems have been conducting cyber offense against one another and sharpening their skills for at least a decade, but they were usually discrete about it (Cavelty, 2012). In September 2010, however, the Stuxnet worm marked a turning point in these governmental cyber operations.

Gradually over some months, the public learned that apparently (although the federal government declined to acknowledge it) the U.S. and Israel had engineered a specialized computer worm called Stuxnet and inserted it into the control software for Iran's nuclear fuel centrifuges. Stuxnet destroyed some centrifuges, deceived the operations of others, and set back Iran's nuclear program by several years (Broad,

Markoff, & Sanger, 2011; Denning, 2012). Other hacking revelations soon followed, including Google's admission in January 2010 that it had been hacked by elements of the Chinese government (Harris, 2014b). In October 2014, commercial investigators announced that the Google hack had been but one of a massive international espionage operation linked to the Chinese government that over the previous 6 years had broken into nearly 1,000 organizations, planting various types of malware, and stealing data from servers across Asia, Europe, and the U.S. (Gertz, 2014).

China and Russia are leading cyber adversaries of the U.S., but many other nations also are players in the game. One analyst describes recent instances that have been inferred and attributed to certain actors—nations rarely admit cyberespionage—this way:

> In 2009, Canadian security researchers discovered a piece of malware called GhostNet on the Dalai Lama's computers. It was a sophisticated surveillance network, controlled by a computer in China. Further research found it installed on computers of political, economic, and media organizations in 103 countries—basically a who's who of Chinese espionage targets. Flame is a surveillance tool that researchers detected on Iranian networks in 2012; these experts believe the United States and Israel put it there and elsewhere. Red October, which hacked and spied on computers worldwide for five years before it was discovered in 2013, is believed to be a Russian surveillance system. So is Turla, which targeted Western government computers and was ferreted out in 2014. The Mask, also discovered in 2014, is believed to be Spanish. Iranian hackers have specifically targeted U.S. officials. There are many more known surveillance tools like these, and presumably others still undiscovered. (Schneier, 2015)

In May 2014, the new Counter Intelligence and Export Controls Section in the DoJ's National Security Division (NSD) raised the stakes in the international cyber competition by indicting in absentia and naming five Chinese military officers who were working in a Chinese Army cyberespionage unit. The five were accused of computer hacking, economic espionage, and conspiracy for hacking into six American companies and a labor union and stealing their controlled trade secrets, passwords, emails and other company correspondence, financial statements, cost projections, and research plans (Federal Bureau of Investigation, 2014; Viswanatha, 2014; "Cyber-Espionage Nightmare," 2015). The contrasting positions taken by China, which openly supports its industries with government intelligence operations, and the U.S., which argues that it does not do so, clashed publicly as American companies protested that Chinese cyberespionage was robbing them of their innovations and business models, and damaging their international competitiveness (Brenner, 2014).

In a further milestone of acknowledged international hacking, in August 2014 the Office of Personnel Management (OPM) admitted that several months earlier, the Chinese had broken into its poorly defended networks and stolen security clearance application records of 21.5 million Americans. This loss offers a foreign intelligence operation potential insight into personal details about cleared individuals, including their interests, vulnerabilities, careers, families and friends that could be exploited for recruitment or blackmail (Gault, 2015; Peterson, 2015).

In September 2015, the prospect of more damaging international cyberattacks led to discussions during Chinese President Xi Jinping's state visit to the U.S, in which he pledged that China would no longer pursue the kind of hacking of which the five Chinese officers stood indicted. In November 2015, at the Group of 20 Conference, China, Russia, the U.S., and most of the other world economic powers negotiated an agreement stipulating that they would follow specified "global rules of responsible behavior in cyberspace," for now (Nakashima, 2015).

Before advancements in ICT, adversaries were positioned at a physical distance from one another. To gain and maintain the competitive advantage, more and better information about the unseen adversary needed to be collected. This prompted the need for and reliance on intercepting signals and also on spies. Cyberespionage overcomes the physical separation between adversaries, which prompts some speculation. If secrets are now kept in electronic storehouses, and the adversary is successfully rifling them, does this not threaten the control over these secrets? If so, can there still be espionage as it has been discussed here? Will there be no need for spies if governments can clandestinely reach into their adversaries' information storerooms from a distance and take what they want? When adversaries have developed their cyber abilities well enough to reach into even the most strongly defended systems and pluck out the secrets, why will they need spies?

### Globalization

Before 1989 ushered in the beginning of the Soviet Union's collapse, the U.S. had faced one main adversary for 4 decades. In 2015, there were many adversaries, including non-state actors. Therefore, the current geopolitical context presents a number of economic competitors and potential military adversaries, along with new challenges for countering their espionage attempts.

Adversaries operate within the current meta-context of globalization, which is the move toward integration of markets and interdependence of peoples that is taking place across many dimensions. This move has been accelerating for several decades, fueled by economic trends, advances in ICT, and cheaper transportation (National Intelligence Council, 2008; World Trade Organization, 2008; Steger & James, 2010).

***Economic Globalization***

As globalization has expanded economic interrelationships to include more peoples and more nations, the value of creative and innovative technology-related ideas has increased. For some nations trying to catch up to the world's economic leaders, the value and speed of innovation has made it worthwhile to invest more effort and resources into stealing secrets as a shortcut in their own development (Hannas, Mulvenon, & Puglisi, 2015).[73]

One characteristic of economic globalization that poses a potential security risk is an increase in multinational corporations and worldwide patterns of manufacturing. Corporations routinely plan large-scale projects, such as aircraft development, that include companies from multiple nations that each contribute a specific part or system, while the lead company coordinates the assembly of these parts into a whole. In such projects, sharing design details and material specifications with foreign partners is essential, yet if they might have military uses, American export control laws often prohibit the release of such advanced materials and technical concepts to non-U.S. companies. It can be difficult for an American company to both comply with export control requirements and collaborate effectively with their international partners (Beck, 2000).

For example, in 2006, Boeing Corporation planned to produce the composite plastic fuselage and wings of its new 787 aircraft in Italy and Japan, but these plans were abruptly delayed when Boeing's own engineers argued that the techniques and composite materials that were to be used had originated in secret military research on the B-2 bomber in the 1980s. In order to avoid violating International Traffic in Arms Regulations (ITAR) restrictions, Boeing reanalyzed each part to be used in the aircraft to determine if it had a military origin, and if so, tried to find an analogous part with a commercial origin to replace it. For months, Boeing delayed production while this replacement was done, despite having provided evidence to regulators of other commercial uses for composites that had not been derived from the B-2.

Dual-use technologies are a thorny area subject to judgment calls. Some argue that export control laws are dangerously outdated, that they no longer prevent the global spread of technologies that could be used against the U.S., and that they should be brought into the 21st century because right now, they "reflect a control system designed for the Cold War rather than the new reality of economic globalization" (Gates, 2006).

Other aspects of globalized economic activity that factor into the potential for economic espionage include supply chains that pass through uncontrolled countries, the exposure of proprietary plans and methods to more people and

[73] This source details efforts by the PRC to covertly acquire technology to underwrite its rapid economic development. The authors argue, "While giving due credit to the Chinese people for their ability to produce, China could not have engineered this transformation, [into an world economic leader] nor sustained its progress today, without cheap and unrestricted access to other countries' technology" (Hannas, Mulvenon, & Puglisi, 2015, p.2).

places that adds to the risk of trade secret theft, and the opportunities that global businesses offer to foreign intelligence services to recruit Americans, who may be exposed to their enticements in international business settings (Figliuzzi, 2012). Because modern global business must use ICT networks to exchange sensitive information, it is as vulnerable as any intelligence or government agency to being hacked and having its information stolen (Brenner, 2014).

As discussed earlier, the Arms Export Control Act (AECA), International Emergency Economic Powers Act (IEEPA), and ITAR laws were written in the 1970s, when the sharp distinction between U.S. and foreign persons made sense. At that time, most manufacturing of American products took place in the U.S. and was performed by American citizens. With globalization, this is no longer as true, and sections in these laws that require excluding non-U.S. persons from knowing about or participating in the development of American technologies sharply clash with current expectations for international collaboration and cooperation. People now work in multinational corporations, perform research in universities among multinational students, and take advantage of joint ventures to pool scarce resources and expertise from various countries to manufacture a complex product (Brown, 2009).

***Cultural Globalization***

One of the important impacts of economic globalization is the elimination of barriers, such as tariffs, to encourage free trade across national boundaries. Cultural globalization deemphasizes the importance of national boundaries, which poses a potential threat to allegiance. As the globalization of cultures has advanced with exposure and interaction—in languages, music, literature, art, political aspirations, and shared concerns for the environment—it has invigorated the notion some have proposed since the end of the Cold War that everyone should first of all be "global citizens. . . who have certain rights and responsibilities towards each other by the mere fact of being human on Earth" (Altinay, 2010). In contrast to the economic dimensions of globalization that increase competition, cultural globalization implies diminished competition, and since espionage presupposes a context of competition, such "one-world-ism" is likely to have an impact.

Global citizenship assumes an ethical and political stance in which the social, political, economic, and environmental realities of the world demand that individuals, communities, and nation-states make decisions based first on global considerations. It emphasizes the fundamental interconnectedness of all things and the reduction of cultural distinctions, sees political and geographical boundaries as increasingly irrelevant, and defines global challenges, such as climate change, as beyond the abilities of one nation or a small group of nations to solve. A global citizen subsumes his or her identity as a citizen of a particular place beneath an identity in the global community. Organizations, conferences, educational curricula, and spokespersons devote themselves to encouraging global

citizenship.[74] One advocate writes, "as a result of living in a globalized world, we understand that we have an added layer of responsibility [in addition to national identities and allegiances]; we also are responsible for being members of a world-wide community of people who share the same global identity that we have" (Israel, 2012).

Individuals who conceived of their espionage as taking place on a higher moral plane, more admirable than loyalty to one nation, are not only a result of modern globalization. Some earlier spies also felt this way. For example, Theodore Hall, an American physicist who worked on the Manhattan project, spied briefly for the Soviets and gave away American nuclear secrets at the end of World War II. He explained that he acted from a higher responsibility, as a citizen of the world, to even up the sides in the Cold War. By helping the Soviets develop their nuclear bomb, he thought he would reduce the danger of nuclear war. He fled prosecution in the U.S. and lived out his life in England (Cowell, 1999).

The claims for global citizenship highlight how much espionage, as it has been conducted in the era of national sovereignty, depends on the existence of competing nation-states, and how much countering espionage depends on those states to command the exclusive allegiance of their citizens. As globalization continues, will the knitting together of peoples in interconnected and overlapping configurations no longer defined exclusively by national boundaries diminish espionage and the attempt to enlist agents to work against their countries? Or, will it simply redefine the players who will undertake espionage in different competing configurations?

***Impact of the Internet***

From 2000 to 2010, the number of global Internet users rose from 413 million to 2.03 billion. By January 2015, that number had risen to more than 3 billion and the rate of increase was accelerating. Already in 2010, almost 30 percent of the world's population had access to computers. There were 1 billion Google searches performed every day, and 2 billion videos were viewed daily on YouTube. By January 2015, 40% of the world's population had Internet access, 51% used mobile communications devices such as cell phones, and 29% had active social media accounts (Kemp, 2015; Internet Live Stats, 2015).

The Internet has been both a product of and catalyst for globalization. It connects computer users around the world, and enables business transactions, consumer

---

[74] Global citizenship is not a recent idea. One author points out that Gouverneur Morris, a delegate to the Constitutional Convention in Philadelphia, criticized "citizens of the world" from the floor of the convention on August 9th, 1787. The convention record noted, "As to those philosophical gentlemen, those Citizens of the World as they call themselves, He owned he did not wish to see any of them in our public Councils. He would not trust them. The men who can shake off their attachments to their own Country can never love any other. These attachments are the wholesome prejudices which uphold all Governments. Admit a Frenchman into your Senate, and he will study to increase the commerce of France; An Englishman, and he will feel an equal bias in favor of that of England." *Notes on the Debates in the Federal Convention". Yale University Avalon Project. http://avalon.law.yale.edu/18th_century/debates_809.asp*

searches, breaking news, and electoral politics, and it allows global participation in sports, entertainment, and public tragedies or triumphs. It allows people who move from their homelands to stay connected to family and friends. Access to the Internet softens the break in ties that immigrants and migrants face, and provides another step toward becoming a global citizen (Herbig, 2008a).

This is the emerging context in which espionage is taking place: ICT, globalization, and increasing reliance on the Internet. As an FBI counterintelligence official noted during a 2014 Congressional hearing, "Long gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it, where modern technology now enables global access and transmission instantaneously" (Coleman, 2014). "Cyber is now part of every mission," an intelligence official explained. "It's not a specialized, boutique thing" (Miller, 2015).

## IMPLICATIONS OF THIS CONTEXT FOR REVISIONS TO THE ESPIONAGE STATUTES

The first part of this report described characteristics of 209 American spies and trends in their activities. The second part explored the five types of espionage those 209 people committed. These five types of espionage are related to one another, but they are not identical. The intent in describing the five types in some detail is to make a case that espionage is not limited to the classic type usually described, but includes leaks, foreign agent activities, violations of export control laws, and economic espionage. Not only in classic espionage but in these other types as well, the U.S. is losing valuable controlled information, ideas, technologies, and plans, and is seeing its economic advantages and national security diminished.

Given this proliferation of types of espionage, along with the transformations in context caused by ICT and globalization, the need to re-think and revise the legal statutes that apply to espionage in the U.S. becomes even more compelling. This report concludes with an overview of possible approaches to revising the espionage statutes.

### Revise Title 18 U.S.C. § 792 through 798

The most narrowly focused revision would consider the recommendations of legal scholars and judges[75] to fix the inconsistencies and ambiguities in the espionage statutes (Title 18 U.S.C. § 792 through 798). Given that these important provisions are based on laws from 1917 and were updated most completely in 1950, at a minimum they need further updating. For example, Harold Edgar and Benno C. Schmidt, Jr., writing in their essay on espionage law in 1973, pointed to subsections (d) and (e) of Section 793 as especially problematic. These subsections are:

> (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails

[75] See the statement by Judge T.S. Ellis in United States District Court for the Eastern District of Virginia (2006). Memorandum opinion, United States of America v. Steven J. Rosen and Keith Weissman.

> to deliver it on demand to the officer or employee of the United States entitled to receive it~ or
>
> (e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . .
>
> shall be fined not more than $10,000 or imprisoned not more than ten years or both.

Edgar and Schmidt closely read the legislative record for the Congressional debates that produced the original Espionage Act in 1917, and also studied the debates during the last major update in 1950. The authors cited the "hopeless imprecision" of these two subsections and wrote, "There is an additional, fundamental problem. . . . the legislation is in many respects incomprehensible." They outlined five serious problems in these subsections that cause inconsistency and confusion for those trying to apply them.

(1) Is publication a "communication" within the meaning of the subsections, and are communications or retentions incident to publication criminal?

(2) What degree of culpability is required by the term "willfully"? Can the word be given a meaning narrow enough to sustain the constitutionality of the prohibitions on communication or retention in light of the vagueness of the phrase "related to the national defense"?

(3) What constitutes protected "information" under the subsections, and what culpability is required before its transfer is criminal?

(4) What makes a piece of paper containing defense information a "document" or other enumerated item for purposes of the subsections?

(5) What does "not entitled to receive it" mean for purposes of the communication and retention offenses? (Edgar & Schmidt, Jr., 1973)

These and other questions have produced many of the legal issues illustrated by cases discussed in this report, including whether leaks to the press constitute acts of espionage or something else, how to demonstrate that a person's motivation to

act was "willful," or how classification of information relates to these provisions when it did not yet exist in 1917.

Sorting out and clarifying the issues raised just in these two subsections could greatly improve the espionage statutes. Judge T. S. Ellis III, who presided over the prosecution of Rosen and Weissman wrote,

> The conclusion that the statute [referring to Section 793] is constitutionally permissible [as his opinion does so conclude,] does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether a more carefully drawn statute could better serve both the national security and the value of public debate. Indeed, the basic terms and structure of this statute have remained largely unchanged since the administration of William Howard Taft. The intervening years have witnessed dramatic changes in the position of the United States in world affairs and the nature of threats to our national security. The increasing importance of the United States in world affairs has caused a significant increase in the size and complexity of the United States' military and foreign policy establishments, and in the importance of our nation's foreign policy decision making. Finally, in the nearly one hundred years since the passage of the Defense Secrets Act [passed in 1911, it was the forerunner of the Espionage Act of 1917] mankind has made great technological advances affecting not only the nature and potential devastation of modern warfare, but also the very nature of information and communication. These changes should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations. (United States District Court for the Eastern District of Virginia, Memorandum opinion, 2006)

### Revise Espionage-related Statutes to Reflect Cyber Capabilities, Globalization, and the Internet

By taking Judge Ellis's observation to heart, broader and more ambitious revisions to all of the most commonly applied espionage statutes[76] could be undertaken to eliminate inconsistencies and frame better laws that reflect the current context of cyber capabilities, the Internet, and globalization. For example, Stephen I. Vladeck, a professor of law, suggested to a House Committee at a 2010 hearing about

[76] That is, Title 18 U.S.C. § 793, 794, 798 and Title 50 U.S C. § 783, as well as the other relevant statutes used in espionage offenses, discussed earlier.

WikiLeaks that the Espionage Act causes "problematic uncertainty" in at least five ways that could and should be addressed by reformers. These include:

(1) Although intended to deal with classic espionage, that is, "using spies to collect information about what another government or company is doing or intends to do," the language of the Espionage Act does not require either "a specific intent to harm the national security of the United States, or to benefit a foreign power." In its vagueness, three crimes end up being prosecuted under the one statute: "classic espionage, leaking, and the retention or redistribution of national defense information by private citizens."

(2) The Espionage Act does not focus only on the initial offender's action, but criminalizes each subsequent person who "knowingly disseminates, distributes, or even retains [a piece of] national defense information." This overly broad application complicates sorting out how leaks to the press should be considered.

(3) The mental state specified in the Espionage Act used to determine intentionality is that the person acted "willfully", but various courts have ruled that other mental states not specified in the Espionage Act can be required as well, including a "bad faith purpose", which adds more complexity to an already complex statute.

(4) The Espionage Act may interfere with the current Federal Whistleblower Protection Act, which does not address the potential conflict with the Espionage Act for those to whom a whistleblower discloses classified information.

(5) The Espionage Act does not acknowledge the possibility that information may be improperly deemed classified or otherwise sensitive by the government, despite the common understanding that this can occur.

Vladeck's suggestions, in part, reflect those of many commentators on the need for a specific law that applies to leaks of classified information to the press. The espionage statutes are a crude fit for leaks, a disjuncture that has prompted charges of unfairness from persons who see themselves as acting as whistleblowers (Epstein, 2007; United States Senate Committee on the Judiciary, 2010; Barandes, 2008).

Another issue for revision is the disappearing ability to distinguish between section 793, in which the recipient is specified to be "anyone not authorized to receive" the information, and section 794, which specifies that the recipient must be any foreign government, or an agent or group of such a government. Proving a nexus to a foreign entity, however, becomes ever more difficult in an era of multinational corporations and global manufacturing, which offer many legitimate reasons for transmitting sensitive information. Also, electronic transmission can occur without leaving a trace as to who has received the information. In these circumstances,

investigators often cannot prove, or even discern, that there was a disclosure of controlled information to a foreign recipient. A similar effect is seen in prosecuting trade secret theft. Section 1831 requires a foreign nexus, while section 1832 does not, and cases often end up being prosecuted under section 1832 because the foreign nexus cannot be proven (Brenner, 2014; Cavelty, 2012; Clapper, 2015; Coleman, 2014).

Not surprisingly, the latest major update to the espionage statutes in 1950 did not anticipate the impact of cyber capabilities to create, store, and transmit information electronically and instantaneously. Taking account of the impact of ICT on current espionage, as well as its impact on developments that may be expected in the future, would be another angle for revision that would improve the espionage statutes and make them more relevant and useful in the 21st century.

For example, when Google chose to make the fact of the Chinese hacking and its investigation into it public, it opened the possibility for the American government to publicly protest the Chinese government's cyber espionage program without having to discuss sensitive sources and methods. "China plays a longer game," one author writes. "Its leaders want the country to become a first-tier economic and industrial power in a single generation, and they are prepared to steal the knowledge they need to do it, U.S. officials say." Defending against such a concerted program involves the NSA, the major communications companies, prominent American corporations, and private security companies in a sharing arrangement both multi-layered and wide-ranging across sectors of the economy. Americans who could support such an international cyberespionage effort by becoming spies for the Chinese would face only the antique espionage statutes that were framed a century ago (Harris, 2014a).

### Reconcile Statutes that Apply to the Five Types of Espionage

The broadest approach that could be taken to revise the espionage statutes would be to consider the statutes that currently are used to prosecute all five types of espionage and undertake an effort to reconcile inequities, eliminate gaps or overlaps, and create more consistency in the legal response to activities that are similar, even though they take place in different spheres. The DoJ NSD has been investigating and assisting with prosecutions of cases across an array of types of espionage for a decade, as the Assistant Director explained to Congress in 2008: "the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons" (United States House of Representatives Committee on the Judiciary, 2008). Testifying at the same Congressional hearing but speaking specifically about Chinese espionage activities, Larry Wortzel, chairman of the U.S.-China Economic and Security Review Commission, made a similar point:

> Indeed, my own view is that today it is often difficult to distinguish between what we define as espionage related to the national defense under the Espionage Act (18 USC 792-8), and economic espionage or the theft of proprietary information and trade secrets covered by the Economic Espionage Act (18 USC 1831-9). Indeed, for American companies and for the national defense of the United States, the impact of espionage can be the same, robbing U.S. companies of the costs of their research, giving technology with military application to China's armed forces, and undermining the security of American military personnel and our nation. (United States House of Representatives Committee on the Judiciary, 2008)

The laws that govern each of the five types are usually different and focused on the distinctive aspects of each crime. The professionals working in each area—case officers, lawyers, investigators, judges—often specialize in one particular type of espionage crime, mastering its own complexities. The communities of interest that have the most at stake when an American gives away or sells information in an act of one of the five types of espionage are distinct. The Intelligence Community, for example, with its reliance on classified information and clandestine sources and methods, differs considerably from the corporate community focused on economic advantage, innovation, and ownership of IP. The people who leak government information to and from the press to the rest of the world, including adversaries and competitors, often differ dramatically in motive from those who agree to serve as agents of a foreign power by collecting information clandestinely in the U.S., and they differ yet again from those who try to profit by selling American export controlled technologies. Each of these five types of espionage results in damage to the U.S. in various but cumulative and multiplying ways. Knowing more about all five types, and considering what they have in common, would be very advantageous to these communities and their practitioners. Thinking about them as one phenomenon could even sharpen our ability to counter them.

# REFERENCES

2012 ClearanceJobs compensation survey (2012). Downloaded from http://www.clearancejobs.com on November 12, 2014.

Accused spy sold nothing secret, defense says. (2010, April 14). Honolulu, HI: *Star Bulletin,* p. 1 [Gowadia].

agent. (n.d.). Dictionary.com Unabridged. Retrieved August 11, 2015, from Dictionary.com website: http://dictionary.reference.com/browse/agent

Agents of Foreign Governments Act. Title 18 U.S.C. § 951. 1938

Altinay, H. (2010, March). The case for global civics. Global Working Papers No. 35. Washington, DC: Brookings Institution.

Amos, C. (2006, December 11). Jilted love, not political intrigue, drove a Salem man to espionage. Salem, OR: *Statesman Journal,* p. 3 [Weinmann].

Anderson, R.H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., Van Wyk, K. (2000). Research on mitigating the insider threat to information systems—#2: Conference Proceedings. Santa Monica, CA: RAND Corporation.

Apodaca, P. (1995, January 24). 2 accused of plot to sell Epogen formula biotech: It's the second foiled industrial espionage attempt in two years involving Amgen's signature drug. Los Angeles: *The Los Angeles Times,* p. D2 [Kota].

Apuzzo, M. (2010, August 27). Federal contractor charged with leaking secrets. New York, NY: *Associated Press* [Kim].

Arrillaga, P. (2011, May 8). How a networking immigrant became a spy. Miami, FL: *The Miami Herald,* p.2 [Kuo, Fondren, Bergersen].

Ashenfelter, D. (2007, April 18). 2 Mich. Men charged as Iraqi spies—For years, they fed info to Hussein regime, U.S. says. Detroit, Michigan: *Detroit Free Press,* p. 3 [Shemami].

Associated Press. (1976, March 1). U.S.-Soviet agent found dead. Washington, DC: *The Washington Post,* p. A1 [Rees].

Associated Press. (2008, August 8). US man who spied for China gets nearly 16 years. Retrieved on August 8, 2008 at http://www.mytimes.com/aponline/us/AP-Chinese-Spies.html [Kuo, Bergersen, Kang].

Associated Press. (2009, June 10). Man who spied for Iraq gets 46 months. Boston: *Boston Globe,* p. 10 [Shemami].

Associated Press. (2010, February 4). Maui spy is competent to stand trial. Maui County, HI: *The Maui Weekly,* p. 1 [Gowadia].

## REFERENCES

Associated Press. (2010, June 25). Judge cuts sentence of Louisiana man who spied for China. New Orleans, LA: *The Times-Picayune,* p. 4 [Kuo, Bergersen, Fondren].

Associated Press. (2011, September 12). Man who tried to export jet to Iran sentenced. Retrieved on August 31, 2012 from http://foxnews.com [Knapp].

Associated Press. (2012, July 20). Syrian agent working in US gets 18 months, admits spying on dissidents during Arab Spring. Washington, DC: *The Washington Post,* p. A5 [Soueid].

Associated Press. (2012, May 7). CIA 'foiled al-Qaida bomb plot' around anniversary of Bin Laden death. London, UK: *The Guardian,* p. 10 [Sachtleben].

Associated Press. (2012, October 1). Terror suspect Babar Ahmad files legal challenge against extradition to US at UK high court. Washington, DC: *The Washington Post,* p. A12 [Abujihaad].

Associated Press. (2012, October 23). CIA 'whistleblower' John Kiriakou jailed for two years for identity leak." London, UK: *The Guardian,* p. 8 [Kiriakou].

Associated Press. (2014, January 31). Gunman's doctor before rampage: 'No problem there.' New York, NY: *New York Post* p. 3 [Alexis].

Baker, P. & Rudoren, J. (2015, November 20). Jonathan Pollard, American who spies for Israel, released after 30 years. New York, NY: *The New York Times,* p. A1 [Pollard].

Bamford, J. (2014, August 22). The most wanted man in the world: Edward Snowden, the untold story. San Francisco, CA: *Wired Magazine.* Retrieved on September 10, 2014 from http://www.wired.com/2014/08/edward-snowden ]Snowden].

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., Trzeciak, R. F. (2006, December). Comparing insider IT sabotage and espionage: A model-based analysis. Pittsburgh, PA: *Software Engineering Institute,* Carnegie Mellon University.

Barakat, M. (2009, September 21). Retired AF officer goes on trial in China spy case. Washington, DC: *The Washington Examiner,* p. 1 [Fondren, Kuo].

Barakat, M. (2011, January 21). US man gets 4 years in prison for attempted spy effort; received $70K from Chinese handlers. Toronto, Canada: *The Canadian Press,* p. 8 [Shriver].

Barandes, L. (2007). A helping hand: Addressing new implications of the Espionage Act on freedom of the press. *Cardozo Law Review,* 29: 371-403.

Barandes, L. (2008). A helping hand: Addressing new implications of the Espionage Act on freedom of the press. Lexington, VA: *Cardozo Law Review*, 29(*1*), p. 371.

Barnes, J. E. & Hodge, N. (2010, July 28). Military probe again targets Manning. New York, NY: *Wall Street Journal,* p. 13 [Manning].

Barisic, S. (2006, December 4). Sailor pleads guilty to espionage. New York, NY: *Associated Press* [Weinmann].

Barrett, D. (2013, September 23). Former FBI agent to plead guilty in leak case. New York, NY: *Wall Street Journal,* p. 6 [Sachtleben].

Beck, M. (2000, Summer). Reforming the multilateral export control regimes. Monterey, CA: *The Nonproliferation review.* Journal of the James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies, Vol. 7*(2),* 91-103.

Beckhusen, R. (2012, December 13). Pentagon warns: 'Pervasive' industrial spying targets U.S. space tech. New York, NY: *Wired Magazine.*

Benkler, Y. (2014, September 8). A case for Edward Snowden's immunity. New York, NY: *The Atlantic* [Snowden].

Bennet, B. (2015, March 6). CIA to create a digital spy division. Los Angeles, CA: *The Los Angeles Times,* p. 12.

Berger, S. (1997, March 24). Memorandum from Samuel Berger, Assistant to the President for National Security Affairs, to George J. Tenet and John P. White, Co-Chairmen, Security Policy Board, Implementation of Executive Order 12968, Attachment. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information [the "Uniform Adjudicative Guidelines"].

Bernstein, L. & Tate, J. (2013, August 22). Bradley Manning says he will live as a woman and seek hormone therapy in prison. Washington, DC: *The Washington Post,* p. 2 [Manning].

Bhattacharjee, Y. (2014, May 5). A new kind of spy. New York, NY: *The New Yorker,* XC(11), 30-36 [Chung].

Black, E. (2004, December 31). Spat erupts between neocons, intelligence community. Forward. Retrieved from http://www.forward.com/main [Franklin].

Blau, E. (1976, March 1). Ex-Mobil Oil engineer linked to Soviet spying is called suicide. New York, NY; *The New York Times,* p. 5 [Rees].

Bowman, M. E. (1995). Prosecuting spies: An uneasy alliance of security, ethics, and law. *Defense Intelligence Journal 4*(57-81).

**REFERENCES**

Boylan, P. & Perez, R. (2005, October 27). Isle man accused of selling secrets. Honolulu, HI: *The Honolulu Advertiser*, p. 1 [Gowadia].

Boylan, P. (2005, October 28). Secrets sold: 'I did it for the money.' Honolulu, HI: *The Honolulu Advertiser*, p. 3 [Gowadia].

Brenner, J. (2014, December 10). The new industrial espionage. *The American Interest*, 10*(3)*. Retrieved on November 11, 2015 at http://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/ .

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli test on worm called crucial in Iran nuclear delay. New York, NY: *International New York Times*, p. 2.

Brock, B. (1987, July). Spying's dirty little secret. *Money, 16*(7), 130-148.

Brown, P. J. (2009, July 29). A midsummer tale of two Chinese spies. Los Angeles, CA: *The Los Angeles Times*, p. 6 [Chung, Shu].

Bruce, J. B & Jameson, W. G. (2013). Fixing leaks: Assessing the Department of Defense's approach to preventing and deterring unauthorized disclosures. Santa Monica, CA: *RAND Corporation.*

Bruce, J. B. (2002, November). Laws and leaks of classified intelligence: Costs and consequences of permissive neglect. Presented at a meeting of the National Security Committee, American Bar Association on November 22, 2002. Arlington, VA. Retrieved on May 21, 2007 from http://cicentre.com/Documents/DOC_Classified _Leaks.htm

Bumiller, E. (2010, July 8). Army leak suspect is turned in, by ex-hacker. New York, NY: *The New York Times*, p. 1 [Manning].

Bunn, M. & Sagan, S. D. (2014). A worst practices guide to insider threats: Lessons from past mistakes. Cambridge, MA: *American Academy of Arts and Sciences.*

Burkett, R. (2013, March). An alternative framework for agent recruitment: from MICE to RASCLS. *Studies in Intelligence, 57*(1) 7-17 (Extracts).

Bush, J D., Dial, A. A., Fisher, J. H. (2013, January 8). Important changes to the federal Economic Espionage Act that protect trade secrets. Atlanta, GA: *Kilpatrick Townsend & Stockton LLP.* Retrieved on August 29, 2015 from http://www.kilpatricktownsend.com/ .

Campbell, D. Spooks admit it in private: Snowden has made them rethink their methods. London, UK: *The Guardian,* p. 3 [Snowden].

Caplan, L. (2013, September 5). Leaks and consequences: Why treating leakers as spies puts journalists at legal risk. Washington, DC: *The American scholar.* Autumn, 2013.

Caught on tape: Selling America's secrets. (2010, February 25). New York, NY: *CBS News.*

Cavelty, M. D. (2012). The militarization of cyberspace: Why less may be better. 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Otis, & K. Ziolkowski, Eds. Tallinn, Estonia: NATO CCD COE Publications.

Chaddock, G. R. (2009, June 6). How an American couple came to be spies for Cuba. *The Christian Science Monitor,* p. 3. [Myers]

Charney, D. L. (2010, Fall/Winter). True psychology of the insider spy. *Intelligencer: Journal of U.S. Intelligence Studies,* 47-54.

Chu, H. (1996, April 10). Retired engineer gets 2 years in Defense espionage case. Los Angeles, CA: *Los Angeles Times,* p. B4. [Charlton]

CI Glossary—Terms and definitions of interest for DoD CI professionals. (2011, May 2). Washington, DC: Office of Counterintelligence (DXC), Defense CI & Humint Center, Defense Intelligence Agency. Retrieved May 5, 2015 from http://fas.org/irp/eprint/ci-glossary.pdf .

Clapper, J. R. (2015, September 10). Statement for the record: Worldwide cyber threats. Provided to the House Permanent Select Committee on Intelligence, Washington, DC.

Clark, C. S. (2015, April 29). CIA chief says overhaul puts spies and analysts 'cheek by jowl.' Washington, DC: *Government Executive.* Retrieved May 7, 2015 from http://www.govexec.com/management/2015/04/cia-overhaul-puts-spies-and-analysts-cheek-jowl-brennan-says/111412/ .

Clark, L. (2010, July 16). Ex-State Department analyst gets life for spying for Cuba. Miami, FL: *The Miami Herald,* p. 4. [Myers]

Coen, J. (2007, April 17). 'Sleeper spy' is found guilty; Des Plaines man to remain in jail. Chicago, IL: *The Chicago Tribune,* p. 2 [Latchin].

Cohn, D. & Caumont, A. (2016, March 31) 10 demographic trends that are shaping the U.S. and the world. Washington, DC: Pew Research Center, retrieved March 16, 2016 at http://www.pewresearch.org/fact-tank/2016/03/31/10-demographic-trends-that-are-shaping-the-u-s-and-the-world/ .

Coleman, R. C. (2014, May 13). Statement before the Committee on the Judiciary, Subcommittee on Crime and Terrorism. United States Senate. At a Hearing Entitled 'Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" Washington, DC.

Coll, S. (2013, April 1). The spy who said too much. New York NY: *The New Yorker, 89*(7): 54 [Kiriakou].

## REFERENCES

Community members spied for Iraq. (2007, April 21). Detroit, Michigan: *The Arab American News*, p. 2 [Shemami].

Congressional notification for authorized public disclosure of intelligence information. (2013, October 8). Directive-type Memorandum (DTM) 13-009. Washington, DC: Deputy Secretary of Defense.

Corcoran, K. (2006, November 6). Convicted in spy case, locked away in secrecy. Indianapolis, IN: *The Indianapolis Star.* Retrieved November 8, 2006 at http://www.indystar.com/apps/pbcs.dll/article. [Shabaan]

Cornell University Law School, (2015). 50 U.S. Code Chapter 35 International Emergency Economic Powers. Cornell, NY. *Legal Information Institute.* Retrieved January 13, 2015 at http://www.law.cornell.edu/uscode/text/50/chapter-35.

Countering espionage, international terrorism, and the counterintelligence insider threat. (2012, May 4). Department of Defense Instruction, Number 5240.26. Washington, DC: Department of Defense.

Cowan, A. L. & Chan, S. (2008, December 30). Ex-Army engineer pleads guilty to spying for Israel. New York, NY: *The New York Times,* p. 3 [Kadish].

Cowell, A. (1999, November 10). Theodore Hall, prodigy and atomic spy, dies at 74. New York, NY: *The New York Times,* p. 16.

Crawford, D. (1998) Volunteers: The betrayal of national defense secrets by Air Force traitors. Washington, DC: Government Printing Office [Buchanan].

Cruz, M. (2010, August 11). Inmate dies on state's death row. San Bernardino, CA: *The Sun News.* Retrieved on July 20, 2015 from http://www.sbsun.com/general-news/20100811/inmate-dies-on-states-death-row#disqus_thread [Diaz].

Currier, C. (2013, July 30). Charting Obama's crackdown on national security leaks. New York, NY: *ProPublica.* Retrieved on June 19, 2015 from https://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks

Cyber-Espionage nightmare: A groundbreaking online-spying case unearths details that companies wish you didn't know about how vital information slips away from them. (2015). Cambridge, MA: *MIT Technology Review* v.13.05.10.

Daugherty, S. (2013a, August 16). Trial begins in Norfolk for ex-sailor accused of spying. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 1. [Hoffman].

Daugherty, S. (2013b, August 17). FBI targeted alleged spy by pretending to date him. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 3 [Hoffman].

Daugherty, S. (2014, February 13). Robert Hoffman: The spy who struck out. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 1 [Hoffman].

Denning. D. E. (2012, July 16). Stuxnet: What has changed? Basel, Switzerland: *Future Internet 4*, pp. 672-687.

Denson, B. (2010, October 1). Former CIA spy Jim Nicholson passed messages to Russians via crumpled napkins, prosecutors allege in new case. Portland, OR: *The Oregonian,* p. 1 [Nicholson].

Denson, B. (2011, May 26). The spy's kid: Jim Nicholson spares his son Nathan from a courtroom confrontation (part 6). Portland, OR: *The Oregonian,* p.10. [6-part series and related articles based on interviews with Nathaniel Nicholson, *The Oregonian,* May 21-May 26, 2011].

Department of Defense Directive. (2014, September 10). The DoD insider threat program. Washington, DC: Office of the Undersecretary of Defense for Intelligence.

Department of Defense Security Institute. (1990, January) The case of Randy Miles Jeffries and Acme Reporting. Richmond, VA: *Security Awareness Bulletin*, 2-90. [Jeffries].

Department of Justice, Office of Public Affairs. (2012, July 20). Virginia man sentenced to 18 months in prison for acting as an unregistered agent of the Syrian government. Washington, DC [Soueid].

Department of Justice, Office of Public Affairs. (2013, June 21). Former workers at Los Alamos National Laboratory plead guilty to Atomic Energy Act violations. Washington, DC [Mascheroni].

Department of Justice. (2008, April 22). Public release: Man arrested for disclosing national defense information to Israel. New York, NY: U.S. Attorney for the Southern District of New York [Kadish].

Department of Justice. (2011, January 13). California man pleads guilty to attempted military exports to Iran. United States District Attorney, District of Delaware [Knapp].

Department of Justice. (2014). Report of the Attorney General to the Congress of the United States on the administration of the Foreign Agents Registration Act of 1938, as amended, for the six months ending June 30, 2015. Washington, DC.

Department of Justice. (2015). Criminal Resource Manual: 2062. Foreign agents registration act enforcement. Washington, DC: Offices of the United States Attorneys.

Department of Justice. (2015). National Security Division: Foreign Agents Registration Act. Washington, DC.

**REFERENCES**

Department of Justice. (2016, February). Former U.S. Nuclear Regulatory Commission employee pleads guilty to attempted spear-phishing cyber-attack on Department of Energy computers. Washington DC: Office of Public Affairs [Eccleston].

Department of the Army. (2010, October 4). Military intelligence: Threat awareness and reporting program. Army Regulation 381-12. Washington, DC: Department of Defense.

Dishneau, D. & Jelinek, P. (2011, December 20). US close to resting case against Manning. New York, NY: *Associated Press*. Retrieved December 20, 2011 from http://news.yahoo.com/us-close-resting-case-against-manning-150522051.html [Manning].

Dolan, M. (1986, January 15). Messenger indicted in Soviet spying case. Los Angeles, CA: *Los Angeles Times,* p. 4 [Jeffries].

Dooley, J. (2009a, January 7). Secrecy tested in Isle spy case. Honolulu, HI: *The Honolulu Advertiser,* p. 2 [Gowadia].

Dooley, J. (2009b, January 25). Judge to rule on spy case evidence. Honolulu, HI: *The Honolulu Advertiser*, p. 2 [Gowadia].

Dooley, J. (2010, April 14). Trial of accused spy begins. Honolulu, HI; *The Honolulu Advertiser*, p. 4 [Gowadia].

Doyle, C. (2014, July 25). Stealing trade secrets and economic espionage: An abridged overview of 18 U. S. Code 1831 and 1832. CRS Report R42682. Washington, DC: Congressional Research Service.

Doyle, C. (2014, July 25). Stealing trade secrets and economic espionage: An overview of 18 U.S.C. 1831 and 1832. Washington, DC: *Congressional Research Service,* R42681.

Dsouza, L. (2012, March 14). Noshir Gowadia father of Chinese stealth technology. Retrieved from *Defence Aviation* on October 5, 2015 from http://www.defenceaviation.com/2012/03/noshir-gowadia-father-of-chinese-stealth-technology.html [Gowadia].

Earley, P. (1997). Confessions of a spy: The real story of Aldrich Ames. New York, NY: Berkley Books, *The Berkley Publishing Group. Penguin Putnam, Inc.*

Earley, P. (2001). All about Aldrich Ames. The Crime Library. Retrieved on January 17, 2003, at http://www.crimelibrary.com/spies/ames/index.htm .

Economic Espionage Act. (1996). Title 18 U.S.C. § 1831-1839.

Economic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats. (2014). Washington DC: *Center for Responsible Enterprise and Trade (CREATe)*

Edgar, H. & Schmidt, Jr., B. C. (1973, May). The espionage statutes and publication of defense information. New York, NY: *Columbia Law Review* 73*(5)*. 929-1087.

Egan, P. (2009, January 3). Prosecutors: Metro area men spied for Saddam; Attorneys, relatives deny charges, say some were coerced by Iraqi regime. Detroit, Michigan: *The Detroit News,* p. 4 [Shemami].

Electronic spycraft is getting easier but more controversial. The old-style human sort is getting harder but more useful. (2015, August 1). London, UK: *The Economist.* p. 20-22.

Elkus, A. (2015, June 18). The devastating breach of US government data highlights an illusory cybersecurity paradox. *Business Insider.* Retrieved on June 19, 2015 from http://www.businessinsider.com/the-opm-breachs-cybersecurity-paradox-2015-6 .

Elmhirst, S. (2009, February 5). China's final frontier. London, UK: *Newstatesman,* retrieved February 6, 2009 from http://www.newstateman.com/print/200902050023 [Chung].

Elsea, J. (2006, December 26). Protection of national security information. Congressional Research Service: *CRS Report for Congress.* Washington, DC: Government Printing Office.

Elsea, J. K. (2013, September 9). Criminal prohibitions on the publication of classified Defense information. Congressional Research Service, R41404. Washington, DC: Government Printing Office.

Engelberg, S. (1986, February 22). Spy for China found suffocated in prison, apparently a suicide. New York, NY: *The New York Times,* p. A3 [Chin].

Epstein, R.D. (2007). Balancing national security and free-speech rights: Why Congress should revise the Espionage Act. *Commlaw Conspectus,* 15: 483-512.

Ex-Boeing engineer guilty in space shuttle spy case. (2009, July 16). New York, NY: *The New York Times,* p. 3. [Chung].

Executive Order 13526. Classified national security information. December 29, 2009.

Executive Order 13587. Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information, October 7, 2011.

Executive Order 9176, Transferring the administration of the act of June 8, 1938, as amended, requiring the registration of agents of foreign principals, from the Secretary of State to the Attorney General, January 19, 1942.

## REFERENCES

Ex-sailor charged in terror case discussed attacking military personnel, prosecutor says. (2007, July 24). Tucson, AZ: *Arizona Daily Star,* p. B3. [Abujihaad].

Federal Bureau of Investigation Eastern District of Virginia. (2012, October 23). Former CIA officer John Kiriakou pleads guilty to disclosing classified information about CIA officer. Washington, DC: United States Attorney's Office [Kiriakou].

Federal Bureau of Investigation Los Angeles Division. (2003). Affidavit in support of a complaint against and arrest warrant for John Jouongwoong Yai and Susan Youngja Yai. Los Angeles, CA [Yai].

Federal Bureau of Investigation Los Angeles Division. (2014, September 8). Former Air Force employee sentenced to prison for retaining stolen government property to sell to a foreign government. Los Angeles, CA: United States Attorney's Office [Orr].

Federal Bureau of Investigation. (2006, September 14). Congressional testimony: Statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation before the House Appropriations Subcommittee on Science, the Department of State, Justice and Commerce, and Related Agencies. Washington, DC: author. [Shabaan]

Federal Bureau of Investigation. (2014). News. Stories: Naval espionage; Stopping a dangerous insider threat. Retrieved December 8, 2014 from http://www.fbi.gov/news/stories/2014/march/naval-espionage-stopping-a-dangerous-insider-threat [Hoffman].

Federal Bureau of Investigation. (2014, May 19). News Blog: Five Chinese military hackers charged with cyber espionage against U.S. Washington, DC: Department of Justice.

Fergusson, I. F. & Kerr, P. K. (2014, January 13). The U.S. export control system and the President's reform initiative. Washington, DC: *Congressional Research Service,* R41916.

Fergusson, I. F. (2009, July 15). The Export Administration Act: Evolution, provisions, and debate. Washington, DC: *Congressional Research Service,* RL31832.

Figliuzzi, C. F. (2012, June 28). Statement for the record before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives, at a hearing entitled "Economic espionage: A foreign intelligence threat to American jobs and homeland security." Washington, DC.

Fishman, S. (2011, July 11). Bradley Manning's army of one. New York, NY: *New York Magazine,* p. 26 [Manning].

Flaccus, G. (2009, June 24). First US economic espionage trial winds down. The Associated Press. Retrieved July 13, 2009 from http://www. Google.com/hosted news/ap/article [Chung].

Flaccus, G. (2009, May 31). First economic espionage trial set in Calif. Washington, DC: *The Washington Post,* p. 2 [Chung].

Flaccus, G. (2010, February 8). Chinese-born spy gets more than 15 years for Calif. Espionage case involving space shuttle. Los Angeles, CA: *Los Angeles Times,* p. 12 [Chung].

Foreign Agents Registration Act. (1938). 22 U.S.C. § 611.

Foreign Press Center Briefing Transcript. (2000, March 7). Intelligence gathering and democracies: The issue of economic and industrial espionage. A briefing by James Woolsey, former director, Central Intelligence Agency. Retrieved on October 19, 2015 from http://fas.org/irp/news/2000/03/wool0300.htm .

Former sailor is convicted in terror case. (2008, March 6). New York, NY: *The New York Times,* p. A1 [Abujihaad].

Former US officer leaked secrets to Chinese girlfriend. (2014, September 18). Washington, DC: *Agence France-Press* [Bishop].

Freeman, C. (2014, December 17). US-Cuba prisoner exchange—who are the 'Cuban five?' London, UK: *The Telegraph,* p. 2 [Guerrero].

Gates, D. (2006, January 22). Separation anxiety: The wall between military and commercial technology. Seattle, WA: *The Seattle Times,* p. 3.

Gault, M. (2015, June 17). Has China learned how to build the perfect U.S. spy? London, UK: *Reuters,* p. 5.

Gentile, C. (2009, June 18). Cuban spies' shortwave radios defy detection. Washington, DC: *Washington Times,* p.1. [Myers]

Gerstein, J. (2006, July 14). A novel-like tale of cloak, dagger unfolds in court. New York, NY: *The New York Sun,* p. 4 [Keyser].

Gerstein, J. (2013, September 23). Ex-FBI agent admits to AP leak. New York, NY: *Politico,* p. 4 [Sachtleben].

Gerstein, J. (2015, February 3). Intelligence agencies tout transparency. New York: NY: *Politico,* p. 2 [Snowden].

Gerth, J. (1989, March 10). Ex-Sergeant's spy case is said to grow in seriousness. New York, NY: *The New York Times,* p. A10 [Conrad, Szabo].

Gertz, B. (1993, February 6). Ex-DIA official pleads guilty in document leak. Washington, DC: *Washington Times,* p. 2 [Hamilton].

## REFERENCES


Gertz, B. (2006, November 23). China bought bomber secrets. Washington, DC: *The Washington Times,* p. 2 [Gowadia].

Gertz, B. (2006, September 18). Enemies. Washington, DC: *The Washington Times,* p. 21 [Chi Mak, Chung].

Gertz, B. (2007, December 12). Engineer indicted on spying. Washington, DC: *The Washington Times,* p. 1 [Gowadia].

Gertz, B. (2009, July 29). Defense analyst in spy case was FBI double agent. Washington, DC: *Washington Times,* p. 1 [Franklin].

Gertz, B. (2014, June 10). U.S. in talks with Snowden on possible plea deal. Washington, DC: *The Washington Free Beacon,* p. 1 [Snowden].

Gertz, B. (2014, October 31). New Chinese intelligence unit linked to massive cyber spying program: Axiom likely a Ministry of State security spy unit. Washington, DC: *The Washington Free Beacon,* p. 3.

Gertz, B. (2015, January 22). NSA details Chinese cyber theft of F-35, military secrets. Chinese hackers pillaged U.S. defense, contractor networks for critical data. Washington, DC: *The Washington Free Beacon,* p. 1 [Snowden].

Gilpin, R. with Gilpin, J. M. (2000). The challenge of global capitalism: The world economy in the 21st century. Princeton, NJ: *Princeton University Press,* chap. 1 *passim.*

Glod, M. (2010, May 25). Former FBI employee sentenced for leaking classified papers. Washington, DC: *The Washington Post,* p. 3 [Leibowitz].

Golden, T. (2002, October 17). Ex-U.S. aide sentenced to 25 years for spying for Cuba. New York: NY: *The New York Times,* p. A6 [Montes].

Golden, T. (2007, October 21). Naming names at Gitmo. New York, NY: *The New York Times,* p. D1 [Diaz].

Goodman, J.D. (2011, October 12). U.S. accuses Virginia man of espionage at Syria protests. New York: *The New York Times,* p. 17 [Soueid].

Gordon, M. (2005, October 28). Grave consequences possible, experts say: Secrets sold: 'I did it for the money.' Honolulu, HI: *The Honolulu Advertiser,* p. 2 [Gowadia].

Greenwald, G, MacAskill, E., & Poitras, L. (2013, June 11). London, UK: *The Guardian,* p. 1 [Snowden].

Grieco, E. M., Acosta, V. D., de la Cruz, G. P., and 5 others. (2012, May) The foreign-born population in the United States: 2010. *American Community Survey Reports.* Washington, DC: United States Census Bureau.

Hammer, D. (2008, May 14). Spy for Chinese pleads guilty. New Orleans, LA: *Times-Picayune*, p. 3 [Kang, Kuo, Bergersen].

Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). Chinese industrial espionage: Technology acquisition and military modernization. New York, NY: *Routledge,* chaps. 7-10 *passim.*

Harnden, T. (2009, October 5). Spying for Fidel: The inside story of Kendall and Gwendolyn Myers. Washington, DC: *Washingtonian Magazine.* Retrieved December 11, 2009 at http://www.washingtonian.com/articles/people/spying-for-fidel-the-inside-story-of-kendall-and-gwen-myers/

Harris, C. R., Jenkins, M., & Glaser, D. (2006, July). Gender differences in risk assessment: Why do women take fewer risks than men? Online journal hosted at University of Pennsylvania: *Judgment and Decision Making,* 73(5): 48-63.

Harris, S. (2010, July 21). Plugging the leaks: Barack Obama hates leaks, and thanks to a tenacious prosecutor, the Justice Department is on its way to setting a record for leak prosecutions. Washington, DC: *The Washingtonian.* Retrieved on July 26, 2011 from http://www.washingtonian.com/articles/people/plugging-the-leaks/

Harris, S. (2014a, May 27). Exclusive: inside the FBI's fight against Chinese cyber-espionage. *Foreign Policy.* Retrieved on November 3, 2015 from http://fpgroup.foreignpolicy.com/ .

Harris, S. (2014b, November 16). Google's secret NSA alliance: The terrifying deals between Silicon Valley and the security state. *Salon.* Retrieved November 30, 2015 from http://www.salon.com/writer/shane_harris/ .

Harris, S. (2015, May 6). CIA's ex-no. 2 says ISIS 'learned from Snowden.' Retrieved on May 15, 2015 from http://www.thedailybeast.com/articles/2015/05/06/cia-s-ex-no-2-says-isis-learned-from-snowden.html .

Hattem, J. (2016, March 30). Former intelligence chairman: More foreign spies in U.S. than ever. Washington, DC: *The Hill.* Retrieved on April 6, 2016 at http://thehill.com/policy/national-security/274704-former-intel-chairman-more-foreign-spies-in-us-than-ever-before.

Herbig, K. L. & Wiskoff, M. F. (2002). Espionage against the United States by American citizens 1947-2001. Monterey, CA: Defense Personnel Security Research Center.

Herbig, K. L. (1994). A history of recent American espionage. In T.R. Sarbin, R.M. Carney & C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal.* Westport, CT: *Praeger.*

## REFERENCES

Herbig, K. L. (2008, December). Allegiance in a time of globalization. Monterey, CA: Defense Personnel Security Research Center.

Herbig, K. L. (2008, March). Changes in espionage by Americans: 1947-2007. Monterey, CA: Defense Personnel Security Research Center.

Heskett, J. (2009, November 4). What is the role of government vis-à-vis capitalism? Working Knowledge. Cambridge, MA: Harvard Business School, retrieved on October 20, 2015 from http://hbswk.hbs.edu/item/6304.html .

Heuer, Jr., R. J. (1992). Compulsive gambling: Background information for security personnel. Monterey, CA: Defense Personnel Security Research Center.

Heuer, Jr., R. J. (2008, May 8). FOUO. Potential counterintelligence risk indicators. Working Paper 08-03. Monterey, CA: Defense Personnel Security Research Center.

Horwitz, S. (2013, September 23). Ex-FBI agent to plead guilty in leak to AP. Washington, DC: *The Washington Post*, p. 9 [Sachtleben].

Hosenball, M. & Strobel, W. (2013, November 7). Exclusive: Snowden persuaded other NSA workers to give up passwords—sources. New York, NY: *Reuters,* p.2 [Snowden].

House of Representatives 110 Congress, Second Session. Committee on the Judiciary. Subcommittee of Crime, Terrorism, and Homeland Security. (2008, January 29). Hearing: Enforcement of federal espionage laws. Washington, DC; U.S Government Printing Office.

Hsu, S. S. (2010, August 28). State Dept. contractor charged in leak to news organization. Washington, DC: *The Washington Post*, p. A14 [Kim].

Hsu, S. S. (2010, July 16). U.S. analyst spying for Cuba gets life in prison; wife gets more than 6 years. Washington, DC: *The Washington Post*, p. A6 [Myers].

Hsu, S. S. (2016, February 2). Former Energy Dept. employee pleads guilty in nuclear secrets sting case. Washington, DC: *The Washington Post,* p. A2 [Eccleston].

Ignatius, D. (2014, June 5). Edward Snowden took less than previously thought, says James Clapper. Washington, DC: *The Washington Post,* p. 12 [Snowden].

Immigration and Customs Enforcement. (2011, September 12). News Releases: California man sentenced to nearly 4 years in prison for attempting to export military items to Iran. Retrieved on August 31, 2012, from http://www.ice.gov/news/releases [Knapp].

Internal review of the Washington Navy Yard shooting. (2013, November 20). A report to the Secretary of Defense. Washington, DC: Under Secretary of Defense for Intelligence.

Internet Live Stats. (2016). Internet users by year. Retrieved on January 14, 2016 from http://www.internetlivestats.com/internet-users/#trend .

Israel, R. C. (2012, Spring/Summer). What does it mean to be a global citizen? *Kosmos: Journal for Global Transformation.* Retrieved on December 21, 2015 from http://www.kosmosjournal.org/featured-topics/living earth/ .

Jaffe, G. & Nakashima, E. (2011, February 2). Leak suspect wasn't fit for war. Washington, DC: *The Washington Post,* p. 1 [Manning].

Jenkins, B. M. (2011). Stray dogs and virtual armies: Radicalization and recruitment to Jihadist terrorism in the United States since 9/11. Santa Monica, CA: *RAND Corporation.*

Joffe-Walt, C. & Spiegel, A. (2012, May 1). Psychology of fraud: Why good people do bad things. Retrieved May 2, 2012 from http://www.npr.org/2012/05/01/151764534/psychology-of-fraud-why-good-people-do-bad-things

Johnson, C. (2008, April 23). Man, 84, is charged with spying for Israel in 1980s. Washington, DC: *The Washington Post,* p. A04 [Kadish].

Johnston, D. (2006, January 21). Former military analyst gets prison term for passing information. New York, NY: *The New York Times,* p. 6 [Franklin].

Joint CIA-FBI press release on arrest of Harold James Nicholson. (1996, November 18). Washington, DC: Federal Bureau of Investigation. [Nicholson].

Kemp, S. (2015, August). Digital, Social, & Mobile in 2015. New York, NY: *We Are Social, Inc.* Retrieved on December 16, 2015 at http://wearesocial.com/us/special-reports/global-statshot-august-2015 .

Kenber, B. (2013, August 28). Nidal Hasan sentenced to death for Fort Hood shooting rampage. Washington, DC: *The Washington Post,* p. A1.

Kennedy, S. & Ruggles, S. (2014, Jan. 08). Breaking up is hard to count: The rise of divorce in the United States, 1980-2010. *Demography 51*(2): 587-598.

Kershaw, S. (2004, February 19). Guardsman charged with trying to spy for Al Qaeda. New York: NY: *The New York Times,* p. 3 [Anderson].

Kiriakou, J. (2014, March 9). I got 30 months in prison. Why does Leon Panetta get a pass? Los Angeles, CA: *The Los Angeles Times,* p. 24 [Kiriakou].

Klopott, F. (2009, October 20). Defense official wants his espionage conviction tossed. Washington, DC: *The Washington Examiner,* p. 5 [Fondren, Kuo].

## REFERENCES

Koerner, B. (2003, July 10). Who must register as a foreign agent? New York, NY: *Slate.*

Kotowoski, J. (2011, January 7). Man sentenced to 5 years for acting as a foreign agent. Bakersfield, CA: *The Bakersfield Californian,* p. 1 [Ali].

Kredo, A. (2010, June 3). Shamai Leibowitz sentenced for leaking FBI secret. Washington, DC: *Washington Jewish Week,* p. 1 [Leibowitz].

Krikorian, G. (2003, February 6). FBI watched spy suspect for 7 years. Los Angeles, CA: *Los Angeles Times*, p. 6 [Yai].

Krotoski M. L. (2009, November). Common issues and challenges in prosecuting trade secret and economic espionage cases. Columbia, SC: *United States Attorneys' Bulletin*, 57(5), pp. 2-23.

Krotoski, M. L. & Harrison, J. (2015, May 8). Reviewing the first foreign economic espionage cases. Washington, DC: *Bloomberg BNA: Patent, Trademark, & Copyright Journal*, 90 (PTCJ 1951), pp. 1-8.

Kundnani, A. & Theoharis, J. (2014, July 23). Breaking the spell of the official terrorism narrative. London, UK: *The Guardian,* p. 3 [Abujihaad].

Kuntz, R. L. (2013, September 1). How not to catch a thief: Why the economic Espionage Act fails to protect American trade secrets. Berkeley, CA: *Berkeley Technology Law Journal*, 28(*4*), 901-932.

LaFraniere, S. (2013, July 20). Math behind leak crackdown: 154 cases, 4 years, 0 indictments. New York, NY: *The New York Times,* p. A3.

Lamothe, D. (2015, January 23). Army details the strange, downward spiral of Fort Hood shooter Ivan Lopez. Washington, DC: *The Washington Post,* p. 4 [Lopez].

Landivar, L. C. (2013). Disparities in STEM employment by sex, race, and Hispanic origin. American Community Survey (ACS) ACS-24, Washington, DC: U.S. Census Bureau.

Leinwand, D. (2008, March 2). FBI follows paper trail to uncover Iraqi spies. McLean, Virginia: *USA Today*, p. 5 [Shemami].

Lentz, P. (1985, June 13). Why spy? Try greed, high tech, lax controls. Chicago, IL: *The Chicago Tribune,* p. A1.

Levine, J. (2012, July 1). Reevaluating ITAR: A holistic approach to regaining critical market share while simultaneously attaining robust national security. Miami, FL: *University of Miami National Security & Armed Conflict Law Review,* Vol. 2*(1),* 1-8.

Lewis, N.A. & Johnston, D. (2009, May 9). U.S. to drop spy case against pro-Israel lobbyists. New York, NY: *The New York Times,* p. 1 [Kadish].

Lewis, N.A. (2008, July 10). Spy cases raise concerns on China's intentions. New York, NY: *The New York Times*, p. A-2 [Bergersen, Kuo, Kang, Chung].

Lichtblau, E. & Risen, J. (2009, April 16). Officials say U.S. wiretaps exceeded law. New York, NY: *The New York Times,* p. 6.

Lichtblau, E. (2009, January 30). Jailed C.I.A. mole kept spying for Russia, via son, U.S. says. New York, NY: *The New York Times,* p. 3 [Nicholson].

Limbago, A. L. (2014, August 20). The more things change...Espionage in the digital age. Retrieved on November 20, 2015 from https://www.endgame.com/blog/more-things-changeespionage-digital-age .

Lindsey, R. (1979). The Falcon and the Snowman. New York, NY: *Simon & Schuster.* [Boyce, Lee].

Lotrionte, C. (2015, Winter). Countering state-sponsored cyber economic espionage under international law. Chapel Hill, NC: *North Carolina Journal of International Law,* 40(*2*), 443-541

Mahony, E. H. (2009, March 5). Judge overturns 1 of ex-sailor's 2 terror convictions. Hartford, CT: *The Hartford Courant,* p. 2 [Abujihaad].

Management of serious security incidents involving classified information. (2014, October 27). ). Department of Defense Directive, Number 5210.50. Washington, DC: Department of Defense.

Manual for Courts-Martial United States (2012 Edition). (2012). Washington, DC: Joint Service Committee on Military Justice. Retrieved on May 5, 2015 from http://www.apd.army.mil/pdffiles/mcm.pdf .

Marimow, A. E. (2013, June 25). A rare look into w Justice Department leak probe. Washington, DC: *The Washington Post*, p. 4 [Kim].

Marimow, A. E. (2014, April 2). Ex-State Dept. advisor Stephen J. Kim sentenced in leak case. Washington, DC: *The Washington Post*, p. 3 [Kim].

Marimow, A. E., & Leonnig, C. D. (2013, December 3). Lawyers for ex-State Dept. worker Stephen J. Kim urge Holder to drop leak charges. Washington, DC: *The Washington Post*, p. 2 [Kim].

Markon, J. & Johnson, C. (2008, April 1). Former Pentagon official pleads guilty to espionage. Washington, DC: *The Washington Post*, p. 4 [Fondren].

Markon, J. (2005a, July 3.) FBI tapped talks about possible secrets. Washington, DC: *The Washington Post,* p. A2 [Franklin].

## REFERENCES

Markon, J. (2005b, October 6). Defense analyst guilty in Israeli espionage case. Washington, DC: *The Washington Post.* p. A4 [Franklin].

Markon, J. (2008, February 12). Defense official is charged in Chinese espionage case. Washington, DC: *The Washington Post,* p. A01 [Bergersen, Kuo].

Markon, J. (2009, May 1). Prosecutors to drop charges against two former AIPAC lobbyists. Washington, DC: *The Washington Post,* p. p. 3 [Franklin].

Macavoy, A. (2008, August 3). Hawaii man accused of helping China design missile. McLean, VA: *USA Today,* p. 7 [Gowadia].

McDonnell, P. J. (2010, February 9). Chinese-born engineer gets 15 years in spying for China. Los Angeles, CA: *Los Angeles Times,* p. 6 [Chung].

McGlone, T. (2006, December 10). Why a patriotic teen joined the Navy and then turned to espionage. Norfolk, VA: *Norfolk Intelligencer-Pilot,* p. 4 [Weinmann]

McGlone, T. (2008a, September 25). Scientist charged with illegally selling technology to China. Hampton Roads, VA: *The Virginian-Pilot,* p. 1 [Shu].

McGlone, T. (2008b, September 30). Physicist charged with selling technology free on bond. Hampton Roads, VA: *The Virginian-Pilot,* p. 3 [Shu].

McGlone, T. (2012, December 12). Former Va. Beach sailor denied bond in spying case. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 5 [Hoffman].

McKenna, M. (2010, August 7). 'Spy' turned to stealth after ADF deal fell through. Melbourne, AU: *The Australian,* p. 1 [Gowadia].

Medina, J. (2007, March 9). Sailor started e-mail on terror, U.S. says. New York, NY: *The New York Times,* p. 9 [Abujihaad].

Meiman, Y. (2008, April 24). The timing/conspiracy theories abound. Retrieved on April 24, 2008 from http://www. Haaretz.com/hasen/spages/977463.html [Kadish].

Miami Spy-hunting. (2000, February 19). Miami, FL: *The Miami Herald,* p. 4 [Alonso, Santos, Linda Hernandez, Nilo Hernandez, Guerrero].

Michigan Technological University. (2015). Research: Export control laws and regulations. Retrieved on September 22, 2015 from http://www.mtu.edu/research/administration/integrity-compliance/export-controls-foreign-nationals/export-control/.

Miller, B. & Pincus, W. (1994, April 22). Wife in spy case cites 'confusion' in interview. Washington, DC: *The Washington Post,* p. D1 [Rosario Ames].

Miller, G. (2013, June 12). The low-profile, tech-savvy intelligence risk. Washington, DC: *The Washington Post,* p. 4 [Manning, Snowden].

Miller, G. (2015, February 23). CIA looks to expand its cyber espionage capabilities. Washington, DC: *The Washington Post,* p. 6.

Molotsky, I. (1985, June 6). Money said to have replaced ideology as main spy motive. New York: NY: *The New York Times,* p. B13.

Monaco, L. O. (2014, February 11). Near-term measures to reduce the risk of high-impact unauthorized disclosures. White House Memorandum. Washington, DC: Assistant the President for Homeland Security and Counterterrorism.

Montlake, S. (2008, April 2). Former Pentagon official pleads guilty in China spy case. Retrieved on April 3, 2008 from http://www.csmonitor.com/World/terrorism-security/2008/0401/p99s01-duts.html [Bergersen, Kuo, Kang].

Morris, T. (2008, August 1). Woman sentenced in Chinese spy case. New Orleans, LA: *Times-Picayune,* p. 6 [Kang, Bergersen, Kuo].

Murphy, J. (2015, March 24). How technology is changing the future of espionage. SOFREP News. Retrieved on November 20, 2015 from http://sofrep.com/40315/technology-changing-future-espionage/ .

Myers, S. L. (2013, October 31). In shadows, hints of a life and even a job for Snowden. New York, NY: *The New York Times,* p. 11 [Snowden].

Nakashima, E. & Tate, J. (2011, December 18). Soldier's gender identity issues are raised in Wikileaks case. Washington, DC: *The Washington Post,* p. 4 [Manning].

Nakashima, E. (2010, July 29). FBI, Justice Dept. help investigate sources of leaked war documents. Washington, DC: *The Washington Post,* p.7 [Manning].

Nakashima, E. (2011, May 8). Bradley Manning is at the center of the WikiLeaks controversy. But who is he? Washington, DC: *The Washington Post,* p. D1 [Manning]. This seminal article is based on 30 interviews with Manning's family and friends.

Nakashima, E. (2014, February 13). NSA employee implicated in Snowden probe resigned, memo says. Washington, DC: *The Washington Post,* p. 5 [Snowden].

Nakashima, E. (2015, November 16). World's richest nations agree hacking for commercial benefit is off-limits. Washington, DC: *The Washington Post,* p. 2.

National Intelligence Council. (2008). Global trends 2025: A world transformed. NIC 2009-003. Washington, DC.

Navy lawyer on trial for leaking info. (2007, May 14). *Morning Edition.* National Public Radio, transcript [Diaz].

**REFERENCES**

Neumeister, L. (2008, April 23). Ex-prosecutor: New arrest shows reach of 1980s spy ring. Washington, DC: *The Washington Post,* p. 3 [Kadish].

Neumeister, L. (2009, May 29). Ex-Army engineer who gave documents to Israelis gets no NY prison term but is fined $50,000. Retrieved on June 5, 2009 from http://www,wpix.com/news/nationworld/sns-ap-us-arrest,0,1950531,print.story [Kadish].

New intelligence agency established. (2014, December 1). Washington, DC: WTOP All News Radio Station.

Newman, A. & Fahim, K. (2008, April 24). New Jersey neighbors sift memory for evidence that a spy was among them. New York, NY: *The New York Times,* p. 4 [Kadish].

Newman, A. (2008, April 23). Ex-engineer for Army is accused of spying for Israel in 1980s. New York, NY: *The New York Times.* p. 2 [Kadish].

Nicks, D. (2010, September 23). Private Manning and the making of Wikileaks. Retrieved March 4, 2011 from http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/print/ [Manning].

Niesse, M. (2010, August 10). Stealth expert guilty of selling secrets to China. San Diego, CA: *San Diego Union-Tribune.* Retrieved on October 5, 2015 from http://www.sandiegouniontribune.com/news/2010/aug/10/stealth-expert-guilty-of-selling-secrets-to-china/ [Gowadia].

Norfolk Naval officer faces court-martial in espionage case. (1995, September 13). Washington, DC: *The Washington Post,* p. D4 [Schwartz].

O'Harrow, Jr., R. (1992, December 29). Man stepping off plane at Dulles is arrested on espionage charges. Washington, DC: *The Washington Post,* p. B1 [Baynes].

O'Sullivan, S. (2011, January 13). Delaware courts: Man admits he violated export ban, pleads guilty. Retrieved on July 11, 2011 from http://www.Delawareonline.com [Knapp]

Office of the National Counterintelligence Executive. (2011, October). Foreign spies stealing U.S. economic secrets in cyberspace. Washington, DC.

Olive, R. J. (2006). Capturing Jonathan Pollard. Annapolis, MD: *Naval Institute Press.*

Osborn, A. & Anishchuk, A. (2013, July 2). Snowden threatens new U.S. leaks, asks numerous countries for asylum. New York, NY: *Reuters,* p. 2 [Snowden].

Pearce, M. (2016, January 20). Where are Iran's billions in frozen assets, and how soon will it get them back? Los Angeles: *Los Angeles Times,* p. 16.

Pentagon man jailed over spying. (2006, January 20). *British Broadcasting Corporation News.* Retrieved from http://news.bbc.co.uk/go/pr/fr [Franklin].

Pentagon officials charged in China espionage case. (2009, May13). Washington, DC: *Agence-France Presse,* p. 1 [Fondren, Kuo, Bergersen, Kang].

Perez, E. (2010, July 17). Spy for Cuba, unrepentant, gets life. New York, NY: *The Wall Street Journal,* p. 4 [Myers].

Peterson, A. (2015, July 13). It's not just OPM: Cybersecurity across the federal government is pretty awful. Washington, DC: *The Washington Post,* p. 6.

Pilkington, E. (2013, July 31). Bradley Manning verdict: Cleared of 'aiding the enemy' but guilty of other charges. London, UK: *The Guardian,* p. 2 [Manning].

Pincus, W. (2009, May 5). A look at the dropping of espionage charges. Washington, DC: *The Washington Post,* p. 8 [Franklin].

Pincus, W. (2010, November 8). Imprisoned former CIA official pleads guilty again. Washington, DC: *The Washington Post,* p. 6 [Nicholson].

Pincus, W. (2013, July 9). Questions for Snowden. Washington, DC: *The Washington Post,* p. A7 [Snowden].

Poole, P. (2010). 10 failures of the U.S. government on the domestic Islamist threat. Washington, DC: *The Center for Security Policy* [Mohamed].

Popkin, J. (2013, April 25). Woman indicted in Cuba spy case is in Sweden and out of U.S. reach. Washington, DC: *The Washington Post,* p. A5 [Velazquez].

Potter, D. (2008, November 13). Va. Scientist pleads guilty to China tech sales. New York, NY: *Associated Press,* p. 2 [Shu].

Pozen, D. E. (2013, December 20). The leaky leviathan: Why the government condemns and condones unlawful disclosures of information. *Harvard Law Review* 127*(2)* , 513-635.

Predicting violent behavior. (2012, August). Defense Science Board Task Force Report. Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics.

Prepared statement of Gabriel Schoenfeld. (2010, December 16). ). Hearing before the Committee of the Judiciary, House of Representatives, 111 Congress 2nd Session. "Espionage Act and the legal and Constitutional issues raised by Wikileaks." Washington, DC: U.S. Government Printing Office.

**REFERENCES**

Pressley, S. A. (1998, September 15). 10 arrested on charges of spying for Cuba; Military facilities targeted, FBI alleges. Washington, DC: *The Washington Post,* p. A01 [Alonso, Gari, Linda Hernandez, Nilo Hernandez, Santos].

Protecting the force: Lessons from Fort Hood. (2010, January). Report of the DoD independent review. Washington, DC: Department of Defense.

Raab, S. (1984, November 29). Friend says spy suspect 'hated Communists.' New York, NY: *The New York Times,* p. A2 [Koecher].

Rafalko, F. J. [Ed.]. (no date). Post-World War II to closing the 20th century. A counterintelligence reader, Volume 3. Washington, DC: The National Counterintelligence Executive.

Rakowsky, J. (1995, October 19). Northborough man charged with espionage. Boston: *The Boston Globe,* p. 41 [Kota].

Ratcliffe, R. (2015, July 19). Babar Ahmad returns to UK after being sentenced for supporting terror groups. London, UK: *The Guardian,* p. 6 [Abujihaad].

Recent cases. (2012). Criminal law—economic espionage—ninth circuit upholds first trial conviction under Section 1831 of the Economic Espionage Act of 1996,—*United States v. Chung,* 659 F.3d 815 (9th Cir. 2011), *cert denied,* No. 11-1141, 2012 WL 929750 (U.S. Apr, 2012). Boston, MA: *Harvard Law Review,* 125*(2177),* pp. 2177-2184 [Chung].

Reilly, T. (2009, November). Economic espionage charges under Title 18 U.S.C. § 1831: Getting charges approved and the "foreign instrumentality" element. Columbia, SC: *United States Attorneys' Bulletin,* 57(5), pp. 24-26.

Reporters Committee for Freedom of the Press. (2015). Emily Peterson, Wikileaks and the Espionage Act of 1917. Retrieved on April 22, 2015 from http://www.rcfp.org/browse-media-law-resources/news-media-law/wikileaks-and-espionage-act-1917.

Reitman, J, (2013, December 19). Snowden and Greenwald: The men who leaked the secrets. New York, NY: *Rolling Stone,* p. 1 [Snowden].

Robles, F. & Davis, Julie H. (2014, December 18). U.S. frees last of the 'Cuban Five,' part of a 1990s spy ring. New York, NY: *The New York Times,* p. A17 [Guerrero].

Rogers, R. (2008, November 17). Former Marine outlines secret dossiers; Muslims, Arabs not targeted, FBI says. San Diego, CA: *The San Diego Union-Tribune,* p. B-1 [Maziarz].

Rosenberg, C. (2007a, May 17). Lawyer: U.S. policy shielded list of captives. Miami, FL: *The Miami Herald,* p. 2 [Diaz].

Rosenberg, C. (2007b, May 18). Navy lawyer guilty of spilling secrets. Miami, FL: *The Miami Herald,* p, 4 [Diaz].

Ross, G. (2011, July). Who watches the watchmen? The conflict between national security and freedom of the press. Washington, DC: *National Intelligence University.*

Roth, S. (2001, March 5). Spy prosecution is an intelligence high-wire act. San Francisco, CA: *American Lawyer Media:* The Recorder, p. 3.

Sample, H. A. (2009, November 10). Hearing begins for Maui man accused of being spy. Retrieved on October 5, 2015 from http://comsecllc.blogspot.com/2009/11/hearing-begins-for-maui-man-accused-of.html [Gowadia].

Sanger, D. E. & Peters, J. W. (2013, June 13). A promise of changes for access to secrets. New York NY: *The New York Times,* p. A18.

Sanger, D. E. & Schmitt, E. (2014, February 8). Snowden used low-cost tool to best N.S.A. New York, NY: *The New York Times,* p. A6 [Snowden].

Satterfield, J. (2008, August 26). Roth was warned, lawyers allege: U.S. official told professor he was breaking the law. Knoxville, TN: *Knoxville News Sentinel,* p. 2 [Roth].

Savage, C. & Huetteman, E. (2013, August 21). Manning sentenced to 35 years for leaking government secrets. New York, NY: *The New York Times,* p. A1 [Manning].

Savage, C. (2013a, July 12). Holder tightens rules on getting reporters' data. New York, NY: *The New York Times,* p. A7.

Savage, C. (2013b, August 13). Manning played vital role in Iraq despite erratic behavior, supervisor says. New York, NY: *The New York Times,* p. 2 [Manning].

Savage, C. (2013c, September 23). Former F.B.I. agent pleads guilty in leak to A.P. New York, NY: *The New York Times,* p. A5 [Sachtleben].

Savage, C. (2014, February 7). Ex-State Department contractor pleads guilty in leak case. New York, NY: *The New York Times,* p. 5 [Kim].

Savage, C. (2015, May 7). N.S.A. phone data collection is illegal, appeals court rules. New York, NY: *The New York Times,* p. p. 5 [Snowden].

Savage, C. (2017, January 17). Chelsea Manning to be released early as Obama commutes sentence. New York: *The New York Times,* p. 2 [Manning].

Schehl, M. L. (2015, February 24). Fort Hood soldier shoots four and himself, police say. Washington, DC: *Army Times,* p. 1.

**REFERENCES**

Schmitt, B. (2009, June 10). Sterling Heights man sentenced after spying for Iraq. Detroit, Michigan: *The Free Press,* p. 2 [Shemami].

Schneier, B. (2015, March 2). What the future of government surveillance looks like. Washington, DC: *Defense One.* Retrieved on December 15, 2915 from http://www.defenseone.com/technology/2015/03/what-future-government-surveillance-looks/106425/ .

Scutro, A. (2007, May 16). Navy lawyer says shared info wasn't secret. Navy Times, Retrieved from http://www.navytimes.com/news/2007/05/navy_guantanamo-trial [Diaz].

Secretary of Defense, (2012, October 18). Memorandum: Deterring and preventing unauthorized disclosure of classified information. Washington DC: Author.

Security from within: Independent review of the Washington Navy Yard shooting. (2013, November).Washington DC: Secretary of Defense Independent Review of the Washington Navy Yard Shooting.

Semko, R. (2013, March 21). More on Bishop spy case. Retrieved on May 20, 2014 from http://www.raysemko.com/home/ [Bishop].

Serrano, R. A. & Reza, H. G. (2008, February 12). Orange County man is accused of being a spy. Los Angeles, CA: *Los Angeles Times,* p. 1 [Chung].

Serrano, R.A. (2003, March 2). The Falcon and the Fallout. Los Angeles, CA: *Los Angeles Times,* p. D1 [Boyce].

Shane, S. (2010, December 11). Keeping secrets wikisafe. New York, NY: *The New York Times,* p. WK1.

Shane, S. (2011a, January 13). Accused soldier in brig as Wikileaks link is sought. New York, NY: *The New York Times,* p. A3 [Manning].

Shane, S. (2011b, September 6). Leak offers look at efforts by U.S. to spy on Israel. New York, NY: *The New York Times,* p. A12 [Leibowitz].

Shane, S. (2013a, January 5). Former CIA officer is the first to face prison for a classified leak. New York, NY: *The New York Times,* p. 20 [Kiriakou].

Shane, S. (2013b, June 21). Ex-contractor is charged in leaks on N.S.A. surveillance. New York, NY: *The New York Times,* p. A4 [Snowden].

Shanker, T. (2010, July 9). Loophole may have aided theft of classified data. New York, NY: *The New York Times,* p. 10 [Manning].

Shaw, E. D., Fischer, L. F., & Rose, A. E. (2009, August). Insider threat evaluation and audit. Monterey, CA: Defense Personnel Security Research Center.

Shaw, E., Payri, M., Cohn, M., & Shaw, I. R. (2013). How often is employee anger an insider risk I? Deterring and measuring negative sentiment versus insider risk in digital communications. Daytona Beach, FL: *Journal of Digital Forensics, Security and Law, 8(1):* 39-71.

Shaw, E., & Sellers, L. (2015, June). Applications of the critical-path method to evaluate insider risks. *Studies in Intelligence,* 59*(2):* 41-48.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2012, December). Common sense guide to mitigating insider threats 4th edition. Pittsburgh, PA: *Software Engineering Institute,* Carnegie Mellon University.

Simon, S. (1998, January). The Economic Espionage Act of 1996. Berkeley, CA: *Berkeley Technology Law Journal,* 13(*1/20),* pp. 305-317.

Smith, J. H. (2010, November 30). Prosecute Wikileaks, then reform our espionage laws. Washington DC: *The Washington Post,* p. 14.

Southern Poverty Law Center. (2015, February 12). Age of the wolf: A study of the rise of the lone wolf and leaderless resistance terrorism. Montgomery, AL: Author.

Spiro, P. J. (2008). Beyond citizenship: American identity after globalization. Oxford, UK: *Oxford University Press.*

Spotlight on the Economic Espionage Act. (2012, March 22). Los Angeles, CA: *Quinn Emanuel Urquhart & Sullivan,* retrieved on August 25, 2015 from http://www.jdsupra.com/legalnews/spotlight-on-the-economic-espionage-act .

Statement of Thomas Blanton. (2010, December 16). Hearing before the Committee of the Judiciary, House of Representatives, 111 Congress 2nd Session. "Espionage Act and the legal and Constitutional issues raised by Wikileaks." Washington, DC: U.S. Government Printing Office.

Steger, M. B. & James, P. (2010). "Ideologies of Globalization," in Paul James and Manfred B. Steger, Eds., *Globalization and Culture: Vol. 4, Ideologies of Globalization.* London, UK: *Sage Publications.*

Stein, J. (2010, July 8). Past Russian spies have found post-swap life gets a bit sticky. Washington, DC: *The Washington Post,* p. 16 [Koecher].

Stein, J. S. (2008, April 25). Israel might have many more spies here, officials say. Retrieved April 28, 2008 from http://www. Cqpolitics.com/frame-templates/print_template.html [Kadish].

Sulick, M. J. (2013). American spies: Espionage against the United States from the Cold War to the present. Washington, DC: *Georgetown University Press.*

**REFERENCES**

Tate, J. (2013, August 21). Bradley Manning sentenced to 35 years in Wikileaks case. Washington, DC: *The Washington Post,* p. 3 [Manning].

The DoD insider threat program. (2014, September 30). Department of Defense Directive, Number 5205.16. Washington, DC: Department of Defense.

Theohary, C. A. & Rollins, J. W. (2015, March 27). Cyberwarfare and cyberterrorism: In brief. Washington, DC: *Congressional Research Service.*

The psychology of espionage. (n.d.). Declassified studies in intelligence article. Retrieved March 11, 2015 from http://www.foia.cia.gov/sites/default/files/DOC_0001407031.pdf

Thomas, J. R. ( 2014, January 15). The role of trade secrets in innovative policy. Washington, DC: *Congressional Research Service,* R41391.

Thomas, P., Ryan, J., & Date, J. (2007, March 7). Former Navy sailor charged with passing secrets to Al Qaeda. ABCNews Internet Ventures. Retrieved from http://www.abcnews.go.com [Abujihaad].

Thompson, G. (2009, June 19). Couple's capital ties said to veil spying for Cuba. New York, NY: *The New York Times,* p. 11. [Myers].

Thompson, T. J. (2014). Toward an updated understanding of espionage motivation. *International Journal of Intelligence and Counterintelligence, 27*: 58-72.

Tsukayama, H. (2014, January 19). NSA program defenders question Snowden's motives. Washington, DC: *The Washington Post,* p. 15 [Snowden].

Uniform Code of Military Justice. (2015). Retrieved on May 27, 2015 from http://www.ucmj.us/ .

United States Attorney's Office District of Connecticut. (2007, March 7). Former member of US Navy arrested in Arizona on terrorism and espionage charges. Hartford, CT: District of Connecticut. [Abujihaad].

United States Attorney's Office District of Hawaii. (2014, March 13). Hawaii man pleads guilty to communicating national defense information to an unauthorized person. Honolulu, HI: United States Department of Justice [Bishop].

United States Attorney's Office Eastern District of Virginia. (2014, February 10). Former sailor sentenced to 30 years in prison for attempted espionage. Alexandria, VA: Eastern District of Virginia [Hoffman].

United States Attorney's Office Eastern District of Virginia. (2008, August 8). Press release. New Orleans man sentenced to more than 15 years in prison for espionage involving China. Washington, DC: United States Department of Justice [Kuo].

United States Court of Appeals for the Ninth Circuit, United States of America, Plaintiff-Appellee v. Dongfan Greg Chung, Defendant-Appellant (2011, September 26). Petition for rehearing and for rehearing en banc; Opinion on the appeal [Chung].

United States Department of Commerce. Bureau of Industry and Security. (2015a) Lists of parties of concern: Denied persons list. Retrieved on September 11, 2015 from https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list .

United States Department of Commerce. Bureau of Industry and Security. (2015b) Lists of parties of concern: Entity list. Retrieved on September 11, 2015 from https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list .

United States Department of Defense. Defense Security Service. (2013). Targeting U.S. technologies: A trend analysis of cleared industry reporting, 2014. Quantico, VA.

United States Department of Defense. Defense Security Service. Center for Development of Security Excellence. (2015). Job aids/tools: Counterintelligence awareness. Understanding espionage and national security crimes. Retrieved on September 9, 2015 from http://www.cdse.edu/documents/cdse/ci-jobaidseries-understandingespionage.pdf .

United States Department of Justice Southern District of Indiana. (2006, May 26). Central Indiana man sentenced for working with former Iraqi intelligence officers. Indianapolis, IN: United States Attorney. [Shabaan]

United States Department of Justice, District of Hawaii, Press release. (2011, January 25). Hawaii man sentenced to 32 years in prison for providing Defense information and services to People's Republic of China; Former B-2 bomber engineer helped PRD design stealthy cruise missile. Honolulu, HI [Gowadia].

United States Department of Justice, Press Release. (2009, April 3). Former member of the U.S. Navy Hassan Abu-Jihaad sentenced to 10 years in federal prison for disclosing classified information. Washington, DC [Abujihaad].

United States Department of Justice, United States Attorney Charles M. Oberly, III, District of Delaware. (2011, January 13). California man pleads guilty to attempted military exports to Iran. Washington, DC [Knapp].

United States Department of Justice, United States Attorney Edward H. Kubo, (2006, November 9). Hawaii man indicted for selling national defense secrets to the People's Republic of China. Honolulu, HI [Gowadia].

## REFERENCES

United States Department of Justice. (1996, November 18). Joint CIA-FBI press release on arrest of Harold James Nicholson. Washington, DC: Office of Public Affairs. [Nicholson]

United States Department of Justice. (2008, August 1). Press release. New Orleans woman sentenced to prison for aiding and abetting unregistered agent of China. Washington, DC. [Kang]

United States Department of Justice. (2008, July 11). Press release. Former Defense Department official sentenced to 57 months in prison for espionage violations. Washington, DC. [Bergersen]

United States Department of Justice. (2008, September 3). Retired University of Tennessee professor convicted of Arms Export Violations. Retrieved March 4, 2009, at http://www.usdoj.gov/opa/pr [Roth].

United States Department of Justice. (2009, January 29). Press release. Imprisoned spy and his son indicted on charges of acting as Russian agents and money laundering. Washington DC. [Nicholson].

United States Department of Justice. (2009, July 1). Press release. Retired University professor J. Reece Roth sentenced to four years in prison for Arms Export Control Violations involving citizen of China. Retrieved July 1, 2009 at http://www.justice.gov/opa/pr [Roth].

United States Department of Justice. (2009, September 25). Press release. Jury convicts Defense Department official James W. Fondren Jr. of unlawful communication of classified information and making false statements. Washington, DC [Fondron].

United States Department of Justice. (2010, July 16). Press release. Former State Department Official sentenced to life in prison for nearly 30-year espionage conspiracy. Washington DC: Office of Public Affairs. [Myers].

United States Department of Justice. (2011, October 12). Virginia man accused of acting as unregistered agent of Syrian government and spying on Syrian protestors in America. Washington, DC: *Justice News.* [Soueid].

United States Department of Justice. (2012, July 20). Virginia man sentenced to 18 months in prison for acting as unregistered agent for Syrian government. Washington DC: *Justice News.* [Soueid].

United States Department of Justice. (2015). Criminal Resource Manual at 1123: Introduction to the Economic Espionage Act. Retrieved on January 13, 2015 at http://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act .

United States Department of Justice. (2015). Criminal Resource Manual at 2057: Synopses of key national defense and national security provisions. Retrieved on April 17, 2015 at http://www.justice.gov/usam/criminal-resource-manual-2057-synopses-key-national-defense-and-national-security-provisions .

United States Department of Justice. (2015). Offices of the United States Attorneys. Priority Area: National Security. Counterespionage/ Counter Proliferation Efforts. Retrieved April 23, 2015 at http://www.justice.gov/usao/priority-areas/national-security/counter-espionage-counter-proliferation-efforts

United States Department of Justice District of Hawaii, Press release. (2010, August 9). Noshir Gowadia convicted of providing Defense information and services to People's Republic of China. Washington, DC [Gowadia].

United States Department of Justice. Federal Bureau of Investigation. (2008, September 19). Redacted Affidavit in support of a criminal complaint and arrest warrant for Shu Quan-sheng. Washington, DC [Shu].

United States Department of Justice. Federal Bureau of Investigation. National Security Branch. (2015). Counterproliferation overview. Retrieved on September 19, 2015 from https://www.fbi.gov/about-us/nsb/nsb-brochure and from https://www/fbi.gov/about-us/nsb/counterproliferation-overview

United States Department of Justice. The Eastern District of Virginia. (2008, September 24). Press release. Virginia Physicist arrested for illegally exporting space launch data to China and offering bribes to Chinese officials. Newport News, VA [Shu].

United States Department of State. (2015). A resource on strategic trade management and export controls. Red flags and watch lists: U.S. Embargo reference chart. Retrieved on September 11, 2015 from http://www.state.gov/strategictrade/redflags/

United States Department of State. (2015). State sponsors of terrorism. Retrieved on August 17, 2015 at http://www.state.gov/j/ct/index.htm .

United States Department of State. Directorate of Defense Trade Controls (2015a). Getting started. Retrieved on September 16, 2015 from https://www.pmddtc.state.gov/documents/ddtc_getting_started.pdf.

United States Department of State. Directorate of Defense Trade Controls. (2015b). United States munitions list. Retrieved September 21, 2015 from http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5#se22.1.121_11 >

## REFERENCES

United States Department of the Navy General Court-Martial. (2007, April 23). Defense response to government motions in limine to exclude certain evidence, United States v. Matthew M. Diaz, LCDR, JAGC, USN [Diaz].

United States District Court Central District of California Southern Division. (2009, July 16). United States of America v. Dongfan "Greg" Chung, Memorandum of Decision [Chung].

United States District Court Central District of California. (October 2008). Grand Jury, United States of America, Plaintiff, v. Dongfan "Greg" Chung, Defendant. Indictment [Chung].

United States District Court Eastern District of Michigan Southern Division. (2007, March 28). Indictment: Najib Shemami.

United States District Court for the Central District of California (June 2002). Grand Jury, United States of America, Plaintiff, v. John Joungwoong Yai and Susan Youngja Yai, Defendants. Indictment [Yai].

United States District Court for the District of Columbia. (2004, February 6). United States of America v. Marta Rita Velazquez: Indictment.

United States District Court for the District of Columbia. (2009, June 4). United States of America v. Walter Kendall Myers and Gwendolyn Steingraber Myers: Indictment.

United States District Court for the District of Columbia. (2010, May 28). Affidavit in support of application for search warrant. Stephen Jin-Woo Kim.

United States District Court for the District of Columbia. (2015, April 23). United States of America v. Charles Harvey Eccleston, Indictment. Washington, DC.

United States District Court for the District of Connecticut. (2007). Warrant for arrest, United States v. Hassan Abujihaad a/k/a "Paul R. Hall." [Abujihaad].

United States District Court for the District of Delaware. (2010, July 20). Criminal complaint: United States of America v. Marc Knapp. Wilmington, Delaware [Knapp].

United States District Court for the District of Hawaii. (2007, October 25). United States of America vs. Noshir S. Gowadia. Second superseding indictment. Honolulu, HI [Gowadia].

United States District Court for the Eastern District of Virginia, Alexandria Division. (2001, February 12). United States of America v. Robert Philip Hanssen. Affidavit in support of criminal complaint, arrest warrant and search warrants [Hanssen].

United States District Court for the Eastern District of Virginia. (2005). Criminal complaint, United States of America v. Lawrence Anthony Franklin.

United States District Court for the Eastern District of Virginia. (2005). Superseding indictment, United States of America v. Lawrence Anthony Franklin.

United States District Court for the Eastern District of Virginia. (2005). Motions hearing (reduction of sentence). United States of America v. Lawrence Anthony Franklin.

United States District Court for the Eastern District of Virginia. (2006). Memorandum opinion, United States of America v. Steven J. Rosen and Keith Weissman.

United States District Court for the Eastern District of Virginia. (2008, February 6) United States v. Tai Shen Kuo, Gregg William Bergersen, and Yu Xin Kang: Affidavit in support of criminal complaint, three arrest warrants, and three search warrants.

United States District Court for the Eastern District of Virginia, Alexandria Division. (2009, June 11). United States v. Lawrence Anthony Franklin, Motions hearing: reduction of sentence. Alexandria, VA [Franklin].

United States District Court for the Eastern District of Virginia, Alexandria Division. (2010, October 22). United States of America v. Glenn Duffie Shriver. Statement of Facts. Alexandria, VA [Shriver].

United States District Court for the Eastern District of Virginia, Alexandria Division. (2010, October 22). United States of America v. Glenn Duffie Shriver. Plea Agreement. Alexandria, VA [Shriver].

United States District Court for the Eastern District of Virginia, Alexandria Division. (2011, October). United States of America v. Mohamad Anas Haithan Soueid. Indictment. Alexandria, VA [Soueid].

United States District Court Southern District of Florida. (2007, February 26). United States of American vs. Carlos Alvarez and Elsa Alvarez: United States sentencing memorandum and response to Carlos Alvarez's request for downward departure. [Alvarez].

United States District Court Southern District of Indiana, Indianapolis Division. (2013, October 21). United States v. Donald John Sachtleben. Government's combined sentencing memorandum. Indianapolis, IN [Sachtleben].

United States Fleet Forces Command. (2006, November 30). Public Affairs Office Media Release: Court martial for sailor begins Dec. 4. Norfolk, VA [Weinmann].

United States Government Accountability Office. (2015, June). Report to Congressional Committees. Insider Threats: DOD should strengthen management and guidance to protect classified information and systems. GAO-15-544. Washington, DC.

## REFERENCES

United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence. (2012, June 28). Hearing: Statement of John P. Woods, Assistant Director, U.S. Immigration and Customs Enforcement, National Security Homeland Security Investigations, regarding a Hearing on "Economic espionage: A foreign intelligence threat to American jobs and homeland security." Washington, DC.

United States House of Representatives Committee on the Judiciary. (2008, January 29). Hearing by the Subcommittee on Crime, Terrorism, and Homeland Security: Statement of J. Patrick Rowan concerning "Enforcement of federal espionage laws." Washington, DC.

United States House of Representatives Committee on the Judiciary. (1996, September 16). Report on the Economic Espionage Act of 1996. Washington, DC. Report 104-788.

United States House of Representatives Committee on the Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet. (2014, June 24). Trade secrets: Promoting and protecting American innovation, competitiveness, and market access in foreign markets. Washington, DC. Report 113-97.

United States Immigration and Customs Enforcement. (2011, September 12). California man sentenced to nearly 4 years in prison for attempting to export military items to Iran. Retrieved on August 31, 2012 from http://www.ice.gov/news/releases/1109/110912wilmington.htm [Knapp].

United States Immigration and Customs Enforcement. (2015). Counter-Proliferation Investigations Program: Overview and Mission. Retrieved on January 13, 2015 from http://www.ice.gov/cpi .

United States Senate Committee on Governmental Affairs. (1985, April 16 -18 and 25). Hearing by the Permanent Subcommittee on Investigations: Witness statement by Christopher J. Boyce during a Hearing on "Federal government security clearance programs." Washington, DC [Boyce].

United States Senate Committee on the Judiciary. (2010, May 12). Testimony of Jeffrey H. Smith during a Hearing on "The espionage statutes: A look back and a look forward." Washington, DC.

United States v. Manning, Bradley E., PFC. (2011, December 2). Defense request for article 32 witnesses. Fort Myer, VA: U.S. Army [Manning].[ Despite sections having been blacked out, this list of defense witnesses and the tenor of their potential testimony reveals details of Manning's Army experience.]

Van Cleave, M. K. (2013, Fall/Winter). What is counterintelligence? A guide to thinking and teaching about CI. *The Intelligencer, 20(2).* Falls Church, VA: Association of Former Intelligence Officers.

Venteicher, W. (2013, April 25). Justice Department accuses U.S. citizen of being Cuban spy. Los Angeles, CA: *Los Angeles Times,* p. 3. [Velazquez]

Vise, D. A. (2002). The bureau and the mole: The unmasking of Robert Philip Hanssen, the most dangerous double agent in FBI history. New York, NY: *Atlantic Monthly Press.* [Hanssen].

Viswanatha, A. (2014, October 21). U.S. national security prosecutors shift focus from spies to cyber. New York, NY: *Reuters.* Retrieved on December 10, 2015 from http://www.reuters.com/article/us-usa-justice-cybersecurity-idUSKCN0IA0BM20141021 .

Vladeck, S. I. (2010, December 16). Prepared statement of Stephen I. Vladeck. Hearing before the House of Representatives Committee on the Judiciary, "The Espionage Act and the legal and constitutional issues raised by Wikileaks." Washington, DC.

Volkman, E. (1994). Spies: The secret agents who changed the course of history. New York, NY: *John Wiley & Sons, Inc.*

Walker, P. (2013, July 30). Bradley Manning trial: what we know from the leaked Wikileaks documents. London, UK: *The Guardian,* retrieved on August 20, 2015 from https://www.theguardian.com/world/2013/jul/30/bradley-manning-wikileaks-revelations.

Warner, J. (2014, May 7). Fact sheet: The women's leadership gap; Women's leadership by the numbers. Washington, DC: *Center for American Progress.*

Weaver, J. (2007, February 27). U.S.: Couple shared vital data with Cuba. Miami, FL: *The Miami Herald,* p. 1 [Alvarez].

Weaver, J. (2009, October 13). Convicted Cuban spy's life sentence reduced to 22 years. Miami, FL: *The Miami Herald,* p. 2 [Guerrero].

Weiser, B. & Risen, J. (1998, December 1). The masking of a militant: A special report.; A soldier's shadowy trail in U.S. and in the Mideast. New York, NY: *The New York Times,* p. A18 [Mohamed].

White & Case Technology Newsflash. (2013, January 15). Amendments to the Economic Espionage Act broaden trade secret protection. New York, NY: *White & Case LLP.* Retrieved on August 28, 2015 from http://www.whitecase.com/publications/article/amendments

White House. FOUO. (2014, February 11). Near-term measures to reduce the risk of high-impact unauthorized disclosures. Washington, DC: Government Printing Office.

White, J. (2006, August 10). Sailor from Oregon charged with espionage. Washington, DC: *The Washington Post,* p. 6 [Weinmann].

## REFERENCES

White, J. (2007, March 8). Former sailor accused of providing data to terrorist web site. Washington, DC: *The Washington Post,* p. A8 [Abujihaad].

Whitlock, C. (2005, August 8). Briton used internet as his bully pulpit. Washington, DC: *The Washington Post,* p. A1 [Abujihaad].

Whitlock, C. & Jaffe, G. (2014, April 4). Argument over paperwork sparked shooting spree, witnesses say. Washington, DC: *The Washington Post,* p. 15 [Lopez].

Wilentz, S. (2014, January 19). Would you feel differently about Snowden, Greenwald, and Assange if you knew what they really thought? New York, NY: *The New Republic.* Retrieved on January 31, 2014 from http://www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe [Snowden].

Williams, L. & McCormick, E. (2001, November 4). Al Qaeda terrorist worked with FBI/ex-Silicon Valley resident plotted embassy attacks. San Francisco, CA: *The San Francisco Chronicle,* p. 4 [Mohamed].

Wilshusen, G. C. (2012, June 28). Information security: Cyber threats facilitate ability to commit economic espionage. Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives. Washington, DC: General Accountability Office.

Wiltrout, K. (2006, August 29). Navy lawyer once posted at Cuba base is charged. Norfolk, VA: *The Norfolk Virginian-Pilot,* Retrieved on http://home.hamptonroads.com/stories [Diaz].

Wiltrout, K. (2006a, August 12). Accused spy carried cash, secret files, agents say. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 2 [Weinmann].

Wiltrout, K. (2006b, August 10). Father dismisses "speculation' on espionage charges against sailor. Norfolk, VA: *Norfolk Virginian-Pilot,* p. 2 [Weinmann].

Wiltrout, K. (2007, May 19). Naval officer sentenced to six months in prison, discharge. Norfolk VA: *The Norfolk Virginian-Pilot,* p. 3 [Diaz].

Wise, D. (2012, June 7). Mole-in-training: How China tried to infiltrate the CIA. Washington, DC: *The Washingtonian,* p. 3 [Shriver].

Wittes, B. (2014, May 29). Thoughts on the Edward Snowden interview. Lawfare: Hard national security choices. Retrieved on June 9, 2014 from http://www.lawfareblog.com/2014/05/thoughts-on-edward-snowdens-interview/ [Snowden].

Wood, S. (2001, October). Public opinion of selected national security issues: 1994-2000. Monterey, CA: Defense Personnel Security Research Center.

Wood, S., Crawford, K. S., Lang, E. L. (2005, May). Reporting of counterintelligence and security indicators by supervisors and coworkers. Monterey, CA: Defense Personnel Security Research Center.

Wood, S. & Marshall-Mies, J. C. (2003, January). Improving supervisor and coworker reporting of information of security concern. Monterey, CA: Defense Personnel Security Research Center.

Wood, S. & Wiskoff, M. F. (1992). Americans who spied against their country since World War II. Monterey, CA: Defense Personnel Security Research Center.

World Trade Organization. (2008). Trends in Globalization. Retrieved December 10, 2015 from https://www.wto.org/.../res.../wtr08-2b_e.pdf

Youssef, N. A. (2011, January 28). Probe: Army ignored warnings over soldier. Miami, FL: *Miami Herald*, p. 1 [Manning].

Zimmerman, M. (2014, September 19). Oahu defense contractor sentenced on espionage charges. *Watchdog.org.* Retrieved September 29, 2014 from http://watchdog.org/171751/espionage-related charges/ [Bishop].

# APPENDIX A:

# ESPIONAGE AS AN INSIDER THREAT

The essay that follows is the result of a viewpoint exercise, a way of seeing familiar material anew. Typically, espionage is considered to be one example among several potential threats posed by insiders. These types of insider threats are usually compared and contrasted in order to identify commonalities that can then become the basis for conclusions about insider threat as a phenomenon. Unlike that approach, this exercise started from the viewpoint of espionage and considered how insider threat studies could improve and expand our understanding of espionage. Therefore, the studies included here are not representative of insider threat literature as a whole, but instead, were included because they offer particular help to those interested in espionage.

Insider threats are not new, but the phrase has taken on a variety of meanings over the years. In the 1980s, insider threats were spies who betrayed classified secrets to foreign governments, usually for money. In the 1990s, the definition expanded to include individuals who misused their authorized computer access and committed theft, information technology (IT) sabotage, and cyberespionage. As a result, early countermeasures included systems security, survivable architectures, and user and enterprise activity monitoring (Anderson et al., 2000).

The 9/11 attacks expanded insider threat to include the threat posed by transnational terrorist organizations such as Al Qaeda and its offshoots. The 9/11 hijackers were not Americans, but their example soon attracted adherents and copycats among American citizens. A series of shocks, starting in 2009, amplified concern about threats from Americans with insider access, and further expanded the focus of insider threat to include unauthorized disclosures and workplace violence. Some of the major events included:

- On November 5, 2009, Army psychiatrist Major Nidal Hasan killed 13 people and wounded 43 more on Fort Hood, an Army base in Texas ("Protecting the Force," 2010; Kenber, 2013).
- Starting on February 28 and continuing through July 25, 2010, WikiLeaks published thousands of classified reports and documents, including diplomatic cables and material related to the Iraq War, provided to Julian Assange by Bradley Manning (Shane, 2011; Secretary of Defense, 2012; Executive Order 13587, 2011).
- Starting in June 2013 and ongoing in 2015, various newspapers around the world published excerpts from thousands of documents detailing classified intelligence programs and surveillance provided to them by Edward Snowden, a contractor with the National Security Agency (NSA) (Shane, 2013b; Sanger & Schmitt, 2014; Wilentz, 2014; Bamford, 2014).
- On September 16, 2013, Aaron Alexis, a veteran and Department of Defense (DoD) contractor, fatally shot 12 people and wounded three more at the Washington Navy Yard in Washington, DC ("Internal Review, 2013; Associated Press, 2014; Department of Defense Directive, 2014).

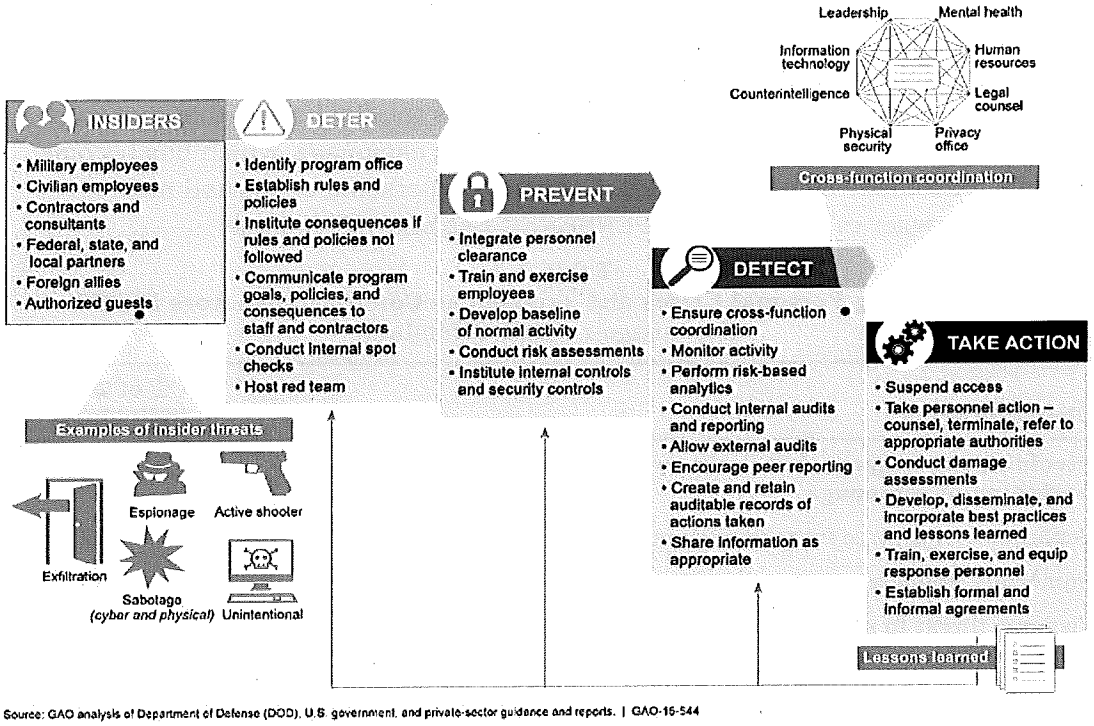
- On April 2, 2014, Army Specialist Ivan Lopez fatally shot three people and wounded 16 others on Fort Hood (Lamothe, 2014; Whitlock & Jaffe, 2014).

Each of these incidents prompted extensive reviews that highlighted gaps in security policies and procedures. Based on those reviews, the government issued policies, set up task forces, and mandated that all federal agencies and military services take steps to detect, deter, and mitigate insider threat behavior (Executive Order 13587, 2011; "Countering Espionage," 2012; "Congressional Notification, 2013; Department of Defense Directive, 2014; Monaco, 2014; " Management of Serious Security Incidents," 2014; "Predicting Violent Behavior, 2012). In response, new fields of academic study and analysis, consulting services, and conference circuits have emerged to address these issues and offer potential solutions.

In some ways, the specific study of espionage is not much advanced by this inclusion in the broad universe of insider threat. In order to frame analytical categories that fit each of the various types of insider threat—and there is no consistent definition from study to study of which types should be included—inevitably these analytical categories become general and somewhat abstract. Beneficially, the categories raise awareness of the dimensions found across the range of insider actions, and allow for comparisons. They also can be applied to the particulars of espionage, but they are limited insofar as they can be applied to the particulars of any and every type of criminal or administrative misconduct that people with insider access may commit. Many findings in current insider threat studies are at such a level of abstraction and generalization that they do not really advance an understanding of espionage itself, or they are obvious and predictable.

As an example, the Government Accountability Office's (GAO) 2015 report to the House of Representatives Armed Services Committee on DoD Insider Threat Programs included a framework of key elements that is reproduced below in Figure A-1. This figure is not shown here because it is deficient, but because it is typical. It lists: potential insiders; potential insider threat behavior; best practices to deter, detect, and mitigate insider threats; and cross-functional stakeholders who must be included in the process. To encompass the breadth of insider threat behavior that ranges from an employee who accidentally attaches a classified document to an email to an active shooter stalking the hallways, the best practices are necessarily open-ended and general (United States Government Accountability Office, 2015). Were one trying to learn how best to respond to the threat of espionage, one would do better to consult the literature on espionage itself than insider threat studies at these high levels of abstraction.

**GAO's Framework of Key Elements To Incorporate at Each Phase of DOD's Insider-Threat Programs**




Source: GAO analysis of Department of Defense (DOD), U.S. government, and private-sector guidance and reports. | GAO-16-544

**Figure A-1 The Government Accountability Office's Summary of Key Elements in Insider Threat Programs**

In other ways, however, insider threat studies can offer valuable insights for students of espionage. Contributions from several areas of insider threat research that are helpful for understanding and responding to espionage are considered in the following sections.

## Personal Crises and Triggers

Descriptions of how people begin to commit an espionage-related offense usually point to individual and environmental preconditions common to most crimes: motive, opportunity, lack of countervailing internal or external constraints, means, and often, a trigger. A trigger is something that happens to propel the person into acting on the intention (Herbig, 1994), or as Thompson writes,

> A trigger is an event, usually negative, which serves as the "straw that breaks the camel's back" and pushes the spy over the edge to espionage. The prospective spy tends to struggle with a crisis for a period of time, during which tension builds up and pushes him/her toward the act.

Once triggered, espionage becomes a viable option. "A trigger merely taps into an existing cauldron of tension and spurs action," (Thompson, 2014). For example, a person who is struggling through the financial and emotional upheavals of a

divorce receives yet another lawyer's bill in the mail, which triggers the decision to commit espionage for financial gain.

Many espionage cases can be modeled in two stages. First, a personal problem develops over time into an impending crisis that becomes the context for planning an act of espionage. Second, some trigger serves as the final straw that motivates the person to try to solve the problem by beginning espionage, which has become the only reasonable solution. Table A-1 reports on personal crises and more immediate trigger events from the PERSEREC Espionage Database.

**Table A-1**
**Precipitating Personal Crises and Triggers as Contextual Factors in 209 Espionage-related Offenders**

| Characteristics | n[77] | % of 209 individuals |
|---|---|---|
| **Precipitating triggers that seem to have caused the beginning of espionage** | | |
| Separation or divorce from significant other | 5 | 2 |
| Immediate financial crisis | 16 | 8 |
| Facing a threat to self or family | 2 | 1 |
| Conflict (interpersonal or job-related) | 16 | 8 |
| **Contextual personal problems or evolving crises within 6 months before date of beginning espionage** | | |
| **Before beginning espionage** | | |
| Separation or divorce from significant other (includes the 5 above for whom this was a trigger) | 19 | 9 |
| Death of family member or close friend | 7 | 3 |
| Diagnosis of terminal illness | 5 | 2 |
| Physical separation from significant other | 8 | 4 |
| Marital problems | 20 | 10 |
| New engagement or marriage | 11 | 5 |
| New significant other | 10 | 5 |
| Began extramarital affair | 20 | 10 |
| Physically relocated | 13 | 6 |
| Reported to have shown financial irresponsibility | 22 | 11 |
| Reported to be having trouble with debt | 68 | 33 |
| Reported to have wanted money, been greedy | 36 | 17 |
| Reported to have shown radically different behavior (from his or her norm) prior to espionage only | 7 | 3 |

[77] A person may have more than one precipitating personal crisis and/or trigger.

| Characteristics | n[77] | % of 209 individuals |
|---|---|---|
| **During espionage** | | |
| Reported to have shown radically different behavior (from his or her norm) prior to and during espionage | 9 | 4 |
| Reported to have shown radically different behavior (from his or her norm) during espionage only | 13 | 6 |
| Reported to have shown unexplained affluence during espionage | 44 | 21 |
| Spending beyond means was reported by others | 23 | 11 |
| Bought a new house | 1 | >1 |
| Bought a new vehicle | 2 | >1 |
| Spending reported and a new house | 5 | 2 |
| Spending reported and a new vehicle | 8 | 4 |
| Spending reported, a new house, + a new vehicle | 5 | 2 |

The preferred research method to explore nuances of timing and motive in an individual's decision to take an irrevocable action, such as beginning to commit espionage, would be to interview the person using a valid and reliable interview protocol. Table A-1, however, was not based on interviews but instead, mostly on open source print materials written after the events. What is lost by using these materials—deeper insights into each person's issues—may be counterbalanced by the breadth of coverage across 209 instances and 7 decades.

Not surprisingly, the themes cluster on basic human issues that can become crises in a person's life: marriage and family, making a home, procuring a livelihood, advancing a career, interacting with co-workers and bosses in a workplace, maintaining financial stability, and ensuring physical health. Table A-1 reinforces the finding that money persists as the predominant motive for espionage-related offenses among Americans: 11% demonstrated financial irresponsibility, 33% struggled with debt, 17% seemed greedy to their coworkers or friends, and 21% displayed unexplained affluence while spying.

Like this report, insider threat studies are based on known use cases. Findings from studies with a broader insider threat focus alert students of espionage of additional factors and patterns they should try to apply specifically to espionage to see if they fit. As an example, CERT published a 2006 study that compared cases of IT sabotage with espionage and made six observations common to both.

Observation #1: Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.

Observation #2: In most cases, stressful events, including organizational sanctions, contributed to the likelihood of insider IT sabotage and espionage.

Observation #3: Concerning behaviors were often observable before and during insider IT sabotage and espionage.

Observation #4: Technical actions by many insiders could have alerted the organization to planned or ongoing malicious acts.

Observation #5: In many cases, organizations ignored or failed to detect rule violations.

Observation #6: Lack of physical and electronic access controls facilitated both insider IT sabotage and espionage (Band, et al, 2006).

Band, et al, analyzed some of the workplace tensions that can escalate into crises that precede IT sabotage or espionage, and provided a useful discussion of the interactions with personal predispositions. The study defined personal predispositions as "relating directly to maladaptive reactions to stress, financial and personal needs leading to personal conflicts and rule violations, chronic disgruntlement, strong reactions to organizational sanctions, concealment of rule violations, and a propensity for escalation during work-related conflicts." These dispositions interact with stressful events, which are not experienced in the same way by everyone. The researchers noted, "what insiders perceived as stressful, how they contributed to the occurrence of stress, and how they reacted to stress were viewed as influenced directly by personal predispositions" (Band et al, 2006).

Shaw, Payri, Cohn, and Shaw (2013) applied some of the insights from the CERT research to recognizing anger in employees and evaluating that anger as a potential insider threat. Their study reported on the development of two observational scales, one for measuring levels of negative sentiment and the other for measuring insider risk. The components of their "Scale of Insider Risk in Digital Communication" help to extend the categories of personal crises and triggers that may be applicable to espionage. The seven components in their scale are:

- *Process*: variables that indicate the extent to which subject behavior that could be directly associated with, or contribute to, the accomplishment of insider actions is present [or] increasing (i.e., preparations, rehearsals, [acquisition of weapons] etc.);
- *Psychological State:* variables that indicate the extent that subject attitudes, beliefs, and feelings are consistent with individuals who have committed insider acts;
- *Personal Predisposition*: variables that indicate the extent to which the subject's observed history, experiences, personal characteristics, and contacts mirror those of previous insider subjects;
- *Personal Stressors*: variables defined as changes in personal or social responsibilities or conditions requiring significant energy for adaptation and do not involve direct workplace or financial issues;

- *Professional Stressors*: variables that include changes in professional, school, and/or work conditions or responsibilities that require significant energy for adaptation, exclusive of financial and personal implications;
- *Concerning Behaviors*: include variables such as violations of workplace or other rules, traditions, laws, policies, or procedures that indicate the extent to which the subject has had difficulty controlling his behavior consistent with expectations, in a manner similar to other insiders; and
- *Mitigating factors*: variables indicating that the subject's level of insider risk may be modified by personal or other characteristics that reduce the level of risk.

Shaw, et al., argued that individuals contemplating an insider crime may follow a critical pathway that can be described in general terms to apply to variety of crimes. In this model, one or more personal stressors, such as "death of a family member, marriage, divorce, births, [or] moves" could become the personal crisis that moves the person along the critical pathway toward espionage or other types of insider actions. The professional stressors here include "graduation, attending a new institution or taking a new job, demotion, termination, promotion, transfer, retirement, consulting jobs, [or] taking side jobs" (Shaw, et al, 2006). Note that stressors can be positive as well as negative conditions that may temporarily de-center a person.[78]

### Indicators of Insider Threat

From the recent dramatic and sometimes violent instances of insider threat has come an urgency to identify and interrupt these threats. This has caused the field of insider threat studies to focus on ways to recognize and interrupt such events by studying indicators in the life and behavior of an insider. These may be general attributes, such as having relatives in a foreign country, or more specific behavioral indicators, which another person would be able to notice. Many insider threat studies provide lists of indicators, usually drawn from cases and described in generalized terms so that they apply to various types of insider threat behavior. For example, in 2008, a PERSEREC study titled "Potential Counterintelligence Risk Indicators" presented indicators from a counterintelligence officer's perspective. These included indicators that a person may be: an attractive target for recruitment by a foreign intelligence service; susceptible to espionage or terrorism; or engaging in espionage, terrorism, or subversive activity (Heuer, Jr., 2008).

Similarly, in 2010, the U.S. Army revised and reissued Army Regulation 381-12, *Military Intelligence: Threat Awareness and Reporting Program (TARP)*, to include potential indicators of espionage, international terrorism, and extremist activity that may pose a threat to DoD or U.S. military operations. These are framed in behavioral terms to enable others to recognize and report them. For example,

[78] Eric Shaw and Laura Sellers (2015) further develop the critical pathway model using case examples from espionage, workplace violence and leaks of classified information.

espionage indicators include: unreported contact with foreign government officials outside the scope of one's official duties, attempts to obtain information for which the person has no authorized access or need to know, and unexplained or undue affluence without logical income source. Examples of indicators of terrorism-related insider threats include: advocating support for terrorist organizations or objectives, and purchasing bomb-making materials. Among the indicators associated with potential extremist activity is someone who expresses a political, religious, or ideological obligation to engage in unlawful violence directed against U.S. military operations or foreign policy (Department of the Army, 2010).

These lists of indicators require individuals to report what they see to a supervisor, security officer, or counterintelligence agent. Yet, there is a general resistance in American culture to reporting the potential misbehavior of others to an authority. In 1994, PERSEREC sponsored research about national security in a national public opinion poll and found the following result.

> The public was asked . . . about what people should do if they saw a person violating security rules. Would they be loyal to their employer—the government—or to their coworker? Respondents were evenly split between those who would immediately report the violation and those who would try to intervene, before reporting, by advising the person to stop the behavior. In other words, they would give the person a chance to change his/her behavior. This is significant, given the fact that cleared individuals are required by regulation to report to authorities any behavior observed among colleagues that may be of security relevance. Presently, the rate of such reporting is extremely low.

In 2003, PERSEREC conducted focus groups to explore the low rate of reporting by co-workers and supervisors (Wood & Marshall-Mies, 2003). One claim by participants stood out: if they recognized that what the person was doing was a serious threat and it was clearly related to security, they would overcome their reluctance and go ahead and report.

This finding led to a second PERSEREC study in 2005, which collected official lists of indicators that observers were directed to report to identify the most serious behaviors based on focus group feedback (Wood, Crawford, & Lang, 2005). An example of a reportable indicator of recruitment by a foreign intelligence service, for example, would be when "you become aware of a colleague having contact with an individual who is known to be, or suspected of being, associated with a foreign intelligence, security, or terrorist organization." A behavior indicating information collection would be when "you find out that a colleague has been keeping classified material at home or at other unauthorized location." Such behaviors demonstrate a clear nexus to security violations, unlike personal behaviors such as alcoholism, absenteeism, or marital problems that people may be hesitant to report (Wood, Crawford, & Lang, 2005).

### Analyzing Organizational Culture

A third contribution from insider threat research that can help better understand espionage is its focus on organizational culture. Insiders, by definition, work and operate inside organizations or institutions. Threats such as workplace violence, fraud, IT sabotage, or the theft of proprietary data take place in an environmental context. Analyzing how organizational structures and cultures encourage or inhibit insider threats has been a major focus and contribution of the research.

In 2009, PERSEREC published an audit tool that organizations could use to evaluate their insider threat risk and take action to reduce those risks. It described the contextual elements of organizations that may magnify the incidence of malicious insider actions, including: economic and social pressures; sector-specific forces, such as technological change; and disruptive forces, such as increased competition or declining resources (Shaw, Fischer, & Rose, 2009). It then pulled together research literature on the most effective approaches that organizations can take to frame their policies so as to mitigate risk, including policies related to: employee screening; monitoring IT systems, critical users, and staff; and termination procedures.

CERT also has published a series of studies focused on how organizations should more effectively mitigate risk. The *Common Sense Guide to Mitigating Insider Threats 4th edition* focuses on IP theft, IT sabotage, and fraud, and offers 19 best practices based on case studies. The advice is directed at certain parts of an organization most responsible for the issue, including human resources, legal, physical security, data owners, IT (and information assurance), and software engineering (Silowash, et al, 2012). Although espionage itself is not discussed in this report, an example relevant to espionage is Practice 8: "Enforce separation of duties and least privileges," which encourages organizations to divide functions between employees and encourage cooperation to minimize solo misuse or abuse of access to systems (Silowash, et al, 2012).

Students of espionage could benefit from systematically analyzing the organizational context in which acts of espionage have occurred. This is not a typical approach in the field because data on the organizations in which espionage-related offenders operated is usually sparse, if not missing entirely. Those who investigate such crimes, usually law enforcement or counterintelligence officials, collect evidence beyond what is relevant for prosecuting the offender from co-workers, supervisors, and organizational policy documentation, but this information is not always made available. Studies that include this material are especially valuable, since having insight into how an organization may have nurtured or hindered a spy, and how it responded to espionage as it was carried out in its offices and hallways, is important for framing effective countermeasures.

A final example presented here is from a 2014 article, *A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes* (Bunn & Sagan, 2014). The focus in this article is on nuclear facilities, and its intended audience is nuclear security

managers, but it draws examples and cases not only from nuclear accidents and security incidents, but also from the experiences of intelligence agencies, the military, bodyguards of political figures, banking and finance, gambling, and the pharmaceutical industry.

One example of a "worst practice" is Lesson #1: "Don't Assume that Serious Insider Problems are NIMO (Not In My Organization)." The authors point out that some businesses, such as diamond mining or gambling, just assume their employees are thieves and treat them accordingly, while many other organizations consider their employees to be part of a carefully screened elite. These latter organizations emphasize loyalty and staff morale to encourage devotion and commitment. The authors suggest intelligence agencies and nuclear organizations usually fall into this category, with their highly educated, vetted staffs. The stress on loyalty, and comparing "our" loyalty favorably against other organizations can lead managers "to falsely assume that insider threats may exist in other institutions, but not in their organizations" (Bunn & Sagan, 2014). The counter example given is of the assassination of President Indira Gandhi in 1984 by the very Sikh bodyguards she most trusted and had insisted should be the only ones to guard her.

A second example that would apply as well to numerous instances of espionage is Lesson #8: "Don't Assume that Security Rules are Followed." This section points out that security procedures and personnel screening policies are often in tension with other goals of an organization, such as maintaining production, meeting deadlines, or generating collegial relationships among employees. Sometimes this tension results in a bending or breaking of a security rule in the name of a higher goal. Often this is done by employees, but sometimes managers do so, too. The management practice of resting on the unexamined assumption that employees are, in fact, following the existing rules can be dangerous, as the examples of security guards at nuclear facilities asleep at their desks or propping open the doors illustrate. Advice to think about what are an organization's incentives for its employees and then aligning them to elicit good security practices, rather than eliciting the evasion of security rules, applies equally well to organizations in which espionage takes place (Bunn & Sagan, 2014).

# APPENDIX B:

# LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

**Table B-1**
**List of the 209 Individuals in this Study and Selected Characteristics**

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Abouelaila | Gladys Ferris | Civilian | 67/00/00 | 69/00/00 | V | **Egypt** |
| Abujihaad | Hassan | Navy | 01/07/19 | 07/03/07 | V | **Al Qaeda** |
| Ali | Amen Ahmed | Civilian | 87/00/00 | 06/09/07 | V | **Yemen** |
| Allen | Michael Hahn | Civilian | 86/00/00 | 86/12/04 | V | **Philippines** |
| Alonso | Alejandro M. | Civilian | 94/00/00 | 98/09/10 | V | **Cuba** |
| Alvarez | Carlos | Civilian | 77/00/00 | 06/01/09 | R | **Cuba** |
| Alvarez | Elsa | Civilian | 82/00/00 | 06/01/09 | R | **Cuba** |
| Ames | Aldrich Hazen | Civilian | 85/04/00 | 94/02/21 | V | **Soviet Union** |
| Ames | Maria del Rosario | Civilian | 92/00/00 | 94/02/21 | R | **Soviet Union** |
| Anderson | Ryan Gilbert | Army | 04/01/00 | 04/02/12 | V | Al Qaeda |
| Anzalone | Charles Lee Francis | Marines | 90/11/00 | 91/02/13 | V | Soviet Union |
| Aragoncillo | Leandro | Marines | 00/08/00 | 05/09/10 | R | **Philippines** |
| Baba | Stephen Anthony | Navy | 81/09/01 | 81/10/09 | V | South Africa |
| Barnett | David Henry | Civilian | 76/10/00 | 80/03/18 | V | **Soviet Union** |
| Baynes | Virginia Jean | Civilian | 90/00/00 | 92/00/00 | R | **Philippines** |
| Bell | William Holden | Civilian | 78/10/00 | 81/06/24 | R | **Poland** |
| Bergersen | Gregg William | Civilian | 07/03/00 | 08/02/11 | R | **China** |
| Bishop | Benjamin Pierce | Civilian | 12/15/14 | 13/03/15 | V | **China** |
| Boeckenhaupt | Herbert William | Air Force | 65/06/00 | 66/10/24 | V | **Soviet Union** |
| Boone | David Sheldon | Army | 88/00/00 | 98/10/10 | V | **Soviet Union** |
| Borger | Harold Noah | Civilian | 59/10/00 | 61/03/03 | R | **East Germany** |
| Boyce | Christopher John | Civilian | 75/05/10 | 77/01/16 | V | **Soviet Union** |
| Brandon | Charles Frederick | Air Force | 77/10/00 | 78/00/00 | V | **Soviet Union** |
| Brown | Joseph Garfield | Civilian | 90/00/00 | 92/12/27 | R | **Philippines** |
| Brown | Russell Paul | Navy | 89/04/00 | 89/07/25 | V | Soviet Union |

[79] The field "Date Began" refers to when the individual began espionage activity. It is expressed as year, month, and lastly day. If only the year is known, the month and day are given as zeros. "Date of Arrest" follows the same date order.

[80] Actual transmission of information to the recipient is noted by bolding the name of the recipient; non-bolded recipients were attempts from perpetrators who did not transmit information.

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Buchanan | Edward Owen | Air Force | 85/05/06 | 85/05/17 | V | East Germany |
| Butenko | John William | Civilian | 63/04/21 | 63/10/29 | R | **Soviet Union** |
| Carney | Jeffrey Martin | Air Force | 83/04/00 | 91/04/22 | V | **East Germany** |
| Cascio | Guiseppe | Air Force | 52/00/00 | 52/09/21 | V | **North Korea** |
| Cavanagh | Thomas Patrick | Civilian | 84/12/00 | 84/12/18 | V | Soviet Union |
| Charlton | John Douglas | Civilian | 93/07/00 | 95/05/00 | V | France |
| Chin | Larry Wu-Tai | Civilian | 52/00/00 | 85/11/22 | R | **China** |
| Chiu | Rebecca Laiwah | Civilian | 83/00/00 | 05/10/28 | R | **China** |
| Chung | Dongfan | Civilian | 79/00/00 | 06/09/11 | R | **China** |
| Clark | James | Civilian | 76/00/00 | 97/10/04 | R | **East Germany** |
| Conrad | Clyde Lee | Army | 74/00/00 | 88/08/23 | R | **Hungary,Czecho-slovakia** |
| Cooke | Christopher Michael | Air Force | 80/12/23 | 81/05/05 | V | **Soviet Union** |
| Cordrey | Robert Ernest | Marines | 84/04/12 | 84/05/16 | V | Soviet Union |
| Davies | Allen John | Civilian | 86/09/22 | 86/10/27 | V | Soviet Union |
| DeChamplain | Raymond George | Air Force | 71/06/05 | 71/07/02 | R | **Soviet Union** |
| Dedeyan | Sahag Katcher | Civilian | 73/03/00 | 75/06/27 | R | **Soviet Union** |
| Diaz | Matthew | Navy | 05/01/15 | 07/01/08 | V | **U.S.** |
| Dolce | Thomas Joseph | Civilian | 79/00/00 | 88/04/16 | V | **South Africa** |
| Drummond | Nelson Cornelious | Navy | 58/00/00 | 62/09/28 | R | **Soviet Union** |
| Dubberstein | Waldo Herman | Civilian | 77/00/00 | 79/00/00 | R | **Libya** |
| Dunlap | Jack Edward | Army | 60/06/00 | 63/00/00 | V | **Soviet Union** |
| Ellis | Robert Wade | Navy | 83/02/09 | 83/02/09 | V | Soviet Union |
| Faget | Mariano | Civilian | 98/12/12 | 00/02/17 | R | **Cuba** |
| Fondren, Jr. | James Wilbur | Civilian | 04/11/00 | 09/05/13 | R | **China** |
| Ford, Jr. | Kenneth W. | Civilian | 04/01/00 | 04/01/12 | V | unknown |
| Franklin | Lawrence Anthony | Civilian | 03/06/26 | 05/05/04 | V | **Israel** |
| French | George Holmes | Air Force | 57/04/05 | 57/04/06 | V | Soviet Union |
| Garcia | Wilfredo | Navy | 85/00/00 | 87/00/00 | R | **Philippines** |
| Gari | George | Civilian | 91/00/00 | 01/08/31 | R | **Cuba** |
| Gessner | George John | Army | 60/12/07 | 61/01/00 | V | **Soviet Union** |

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Gilbert | Otto Attila | Civilian | 82/04/17 | 82/04/17 | R | Hungary |
| Gowadia | Noshir | Civilian | 99/12/12 | 05/10/25 | V | **China, Israel, Germany, Switzerland,** Austria, Lichtenstein, 2 others |
| Graf | Ronald Dean | Navy | 89/00/00 | 89/03/03 | V | unknown |
| Gregory | Jeffrey Eugene | Army | 84/03/00 | 93/04/29 | R | **Hungary,Czecho-slovakia** |
| Groat | Douglas | Civilian | 97/03/24 | 98/04/01 | V | unknown |
| Grunden | Oliver Everett | Air Force | 73/09/28 | 73/11/02 | V | Soviet Union |
| Guerrero | Antonio | Civilian | 91/00/00 | 98/09/12 | R | Cuba |
| Haeger | John Joseph | Navy | 89/10/00 | 89/12/01 | R | Soviet Union |
| Haguewood | Robert Dean | Navy | 86/02/00 | 86/03/04 | V | unknown |
| Hall, III | James William | Army | 82/12/00 | 88/12/21 | V | **East Germany, Soviet Union** |
| Hamilton | Frederick Christopher | Civilian | 91/02/00 | 92/00/00 | V | **Ecuador** |
| Hamilton | Victor Norris | Civilian | 62/00/00 | 63/00/00 | V | **Soviet Union** |
| Hanssen | Robert Philip | Civilian | 79/00/00 | 01/02/18 | V | **Soviet Union** |
| Harper, Jr. | James Durward | Civilian | 75/00/00 | 83/10/15 | R | **Poland** |
| Harris | Ulysses Leonard | Army | 67/02/08 | 67/08/25 | V | **Soviet Union** |
| Hawkins | Stephen Dwayne | Navy | 85/00/00 | 85/08/07 | V | unknown |
| Helmich, Jr. | Joseph George | Army | 63/00/00 | 81/07/15 | V | **Soviet Union** |
| Hernandez | Linda | Civilian | 94/00/00 | 98/09/10 | R | **Cuba** |
| Hernandez | Nilo | Civilian | 92/00/00 | 98/09/12 | R | **Cuba** |
| Hoffman, II | Robert Patrick | Civilian | 12/10/21 | 12/12/06 | R | Russia |
| Hoffman | Ronald Joshua | Civilian | 86/09/09 | 90/06/15 | V | **Japan** |
| Horton | Brian Patrick | Navy | 82/06/00 | 82/09/30 | V | Soviet Union |
| Howard | Edward Lee | Civilian | 84/09/00 | 85/00/00 | V | **Soviet Union** |
| Humphrey | Ronald Louis | Civilian | 76/00/00 | 78/01/31 | V | **Vietnam** |
| Inson | Seivirak | Army | 09/00/00 | 12/06/00 | V | **Cambodia** |
| Irene | Dale Vern | Civilian | 84/08/12 | 84/08/23 | R | Soviet Union |

## APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Jeffries | Randy Miles | Civilian | 85/12/14 | 85/12/20 | V | **Soviet Union** |
| Jenott | Eric O. | Army | 96/00/00 | 96/06/26 | V | **China** |
| Johnson | Robert Lee | Army | 53/02/00 | 65/04/05 | V | **Soviet Union** |
| Jones | Geneva | Civilian | 91/00/00 | 93/08/03 | V | **Liberia** |
| Kadish | Ben-Ami | Civilian | 79/06/05 | 08/04/22 | R | **Israel** |
| Kampiles | William Peter | Civilian | 78/02/00 | 78/08/17 | V | **Soviet Union** |
| Kauffman | Joseph Patrick | Air Force | 60/09/00 | 61/12/00 | R | **East Germany** |
| Keyser | Donald Willis | Civilian | 95/00/00 | 04/09/15 | R | **Taiwan** |
| Kim | Robert Chaegon | Civilian | 96/04/00 | 96/09/24 | V | **South Korea** |
| Kim | Stephen Jin-Woo | Civilian | 09/03/00 | 10/08/27 | V | **U.S.** |
| King | Donald Wayne | Navy | 89/10/00 | 80/30/3 | V | unknown |
| Kiriakou | John C. | Civilian | 07/12/08 | 12/01/23 | V | **U.S.** |
| Knapp | Marc | Civilian | 09/12/24 | 10/07/20 | V | Iran, Russia |
| Koecher | Karel Frantisek | Civilian | 73/02/00 | 84/11/27 | R | **Czechoslovakia** |
| Kota | Subrahmanyam | Civilian | 85/00/00 | 95/10/18 | R | **Soviet Union** |
| Kunkle | Craig Dee | Civilian | 88/12/00 | 89/01/10 | V | Soviet Union |
| Kuo | Tai Shen | Civilian | 07/03/00 | 08/02/11 | R | **China** |
| Lalas | Steven J. | Army | 77/00/00 | 93/05/03 | 9 | **Greece** |
| Latchin | Sami Khoshaba | Civilian | 93/00/00 | 04/08/31 | R | **Iraq** |
| Ledbetter | Gary Lee | Navy | 67/04/00 | 67/05/00 | R | **Soviet Union** |
| Lee | Andrew Daulton | Civilian | 75/05/18 | 77/01/17 | V | **Soviet Union** |
| Lee | Peter H. | Civilian | 85/00/00 | 97/00/00 | V | **China** |
| Leibowitz | Shemai Kedem | Civilian | 09/04/00 | 09/08/00 | V | **U.S.** |
| Lessenthien | Kurt G. | Navy | 96/00/00 | 96/04/22 | V | Russia |
| Leung | Katrina M. | Civilian | 90/04/00 | 03/04/09 | R | **China** |
| Lipka | Robert Stephan | Army | 65/09/00 | 96/02/23 | V | **Soviet Union** |
| Lonetree | Clayton John | Marines | 86/01/00 | 86/12/00 | R | **Soviet Union** |
| Madsen | Lee Eugene | Navy | 79/07/26 | 79/08/14 | V | unknown |
| Mak | Chi | Civilian | 83/00/00 | 05/10/28 | R | **China** |
| Manning | Bradley E. | Army | 09/11/19 | 10/05/26 | V | **U.S.** |
| Martin | Bryan Minkyu | Navy | 10/11/15 | 10/12/01 | V | China |

## APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Martin | William Hamilton | Civilian | 60/08/00 | 61/0000 | V | **Soviet Union** |
| Mascheroni | Marjorie Roxby | Civilian | 07/09/00 | 10/09/17 | R | Venezuela |
| Mascheroni | Pedro Leonardo | Civilian | 07/09/00 | 10/09/17 | V | Venezuela |
| Maziarz | Gary | Marines | 04/00/00 | 06/10/00 | R | **U.S.** |
| Mehalba | Ahmed | Civilian | 03/00/00 | 03/09/29 | R | **Egypt** |
| Millay | William Colton | Army | 11/06/00 | 11/10/28 | V | Russia |
| Miller | Richard William | Civilian | 84/05/00 | 84/10/03 | R | **Soviet Union** |
| Mintkenbaugh | James Allen | Army | 53/06/00 | 65/04/05 | R | **Soviet Union** |
| Mira, F. | Francisco de Asis | Air Force | 82/05/00 | 83/03/25 | V | **Soviet Union** |
| Mitchell | Bernon Ferguson | Civilian | 60/08/00 | 61/00/00 | V | **Soviet Union** |
| Mohamed | Ali Abdelseoud | Army | 89/00/00 | 98/09/10 | V | **Al Qaeda** |
| Montaperto | Ronald N. | Civilian | 83/00/00 | 04/02/04 | R | **China** |
| Montes | Ana Belen | Civilian | 80/00/00 | 01/09/21 | R | **Cuba** |
| Moore, II | Edwin Gibbons | Civilian | 76/12/22 | 76/12/22 | V | Soviet Union |
| Morison | Samuel Loring | Civilian | 84/07/00 | 84/10/01 | V | **United Kingdom** |
| Mortati | Thomas | Civilian | 81/00/00 | 89/12/01 | R | **Hungary** |
| Mueller | Gustav Adolph | Air Force | 49/10/00 | 49/10/00 | V | Soviet Union |
| Murphy | Michael Richard | Navy | 81/06/00 | 81/00/00 | V | Soviet Union |
| Myers | Gwendolyn S. | Civilian | 80/00/00 | 09/06/04 | R | **Cuba** |
| Myers | Walter Kendall | Civilian | 80/00/00 | 09/06/04 | R | **Cuba** |
| Nesbitt | Frank Arnold | Civilian | 89/09/00 | 89/10/14 | R | **Soviet Union** |
| Nicholson | Harold James | Civilian | 94/06/27 | 96/11/16 | V | **Soviet Union** |
| Nicholson | Nathaniel James | Civilian | 06/06/00 | 09/01/29 | R | **Russia** |
| Nour | Almaliki | Civilian | 03/00/00 | 06/10/00 | V | **Al Qaeda** |
| Nozette | Stewart David | Civilian | 09/09/03 | 09/10/19 | R | Israel |
| Oakley | Roy Lynn | Civilian | 06/10/17 | 07/08/02 | V | France |
| Orr | Brian Scott | Civilian | 13/09/00 | 13/11/15 | V | China |
| Ott | Bruce Damian | Air Force | 86/01/09 | 86/02/22 | V | Soviet Union |
| Payne | Leslie Joseph | Army | 74/00/00 | 74/10/00 | V | **East Germany** |
| Pelton | Ronald William | Civilian | 80/01/15 | 85/11/25 | V | **Soviet Union** |
| Peri | Michael Anthony | Army | 89/02/20 | 89/03/04 | V | **East Germany** |

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Perkins | Walter Thomas | Air Force | 68/12/00 | 71/10/21 | R | **Soviet Union** |
| Petersen, Jr. | Joseph Sidney | Civilian | 48/03/01 | 54/10/09 | V | **Netherlands** |
| Pickering | Jeffrey Loring | Navy | 82/00/00 | 83/00/00 | V | **Soviet Union** |
| Pitts | Earl Edwin | Civilian | 87/07/00 | 96/12/18 | V | **Soviet Union** |
| Pizzo, II | Francis Xavier | Civilian | 85/08/11 | 85/08/13 | V | Soviet Union |
| Pollard | Anne Henderson | Civilian | 85/11/00 | 85/11/22 | R | **Israel, China** |
| Pollard | Jonathan Jay | Civilian | 84/06/00 | 85/11/21 | R | **Israel, China** |
| Ponger | Kurt Leopold | Civilian | 49/06/15 | 53/01/14 | R | **Soviet Union** |
| Ramsay | Roderick James | Army | 83/09/00 | 90/06/07 | R | **Hungary,Czecho-slovakia** |
| Rees | Norman john | Civilian | 42/00/00 | 71/0000 | V | **Soviet Union** |
| Regan | Brian Patrick | Air Force | 99/00/00 | 01/08/21 | V | Libya, Iraq, China |
| Rhodes | Roy Adair | Army | 51/12/00 | 57/06/00 | R | **Soviet Union** |
| Richardson | Daniel Walter | Army | 88/01/00 | 88/01/14 | V | Soviet Union |
| Rohrer, G. | Glenn Roy | Army | 58/00/00 | 65/0000 | R | **Czechoslovakia** |
| Rondeau | Jeffrey Stephen | Army | 85/00/00 | 92/10/22 | R | **Hungary,Czecho-slovakia** |
| Roth | John Reece | Civilian | 04/01/00 | 08/05/21 | V | **China** |
| Sachtleben | Donald John | Civilian | 09/00/00 | 12/05/11 | V | **U.S.** |
| Safford | Leonard Jenkins | Army | 67/02/08 | 67/08/25 | V | **Soviet Union** |
| Santos | Joseph | Civilian | 95/00/00 | 98/09/10 | R | **Cuba** |
| Sattler | James Frederick | Civilian | 67/00/00 | 74/0000 | R | **East Germany** |
| Scarbeck | Irvin Chambers | Civilian | 60/12/22 | 61/06/13 | R | **Poland** |
| Schoof | Charles Edward | Navy | 89/10/00 | 89/12/01 | V | Soviet Union |
| Schuler | Ruby Louise | Civilian | 79/05/01 | 83/00/00 | R | **Poland** |
| Schwartz | Michael Stephen | Navy | 92/11/00 | 96/00/00 | 9 | **Saudi Arabia** |
| Scranage | Sharon Marie | Civilian | 83/12/00 | 85/07/11 | R | **Ghana** |
| Seldon | Phillip Tyler | Civilian | 92/11/00 | 96/00/00 | R | **El Salvador** |
| Shaaban | Shaaban Hafed | Civilian | 02/11/00 | 05/03/03 | V | Iraq |
| Shemami | Najeb Elias | Civilian | 02/00/00 | 07/04/17 | R | **Iraq** |
| Sherman | Daniel Max | Civilian | 04/01/00 | 08/04/15 | V | **China** |
| Shriver | Glenn Duffie | Civilian | 04/10/00 | 10/06/24 | R | China |

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Shu | Quan-Sheng | Civilian | 03/01/00 | 08/09/24 | V | **China** |
| Slatten | Charles Dale | Army | 84/02/00 | 84/04/14 | V | Soviet Union |
| Slavens | Brian Everett | Marines | 82/08/31 | 82/09/04 | V | Soviet Union |
| Smith | Richard Craig | Civilian | 81/00/00 | 84/05/04 | V | **Soviet Union** |
| Smith | Timothy Steven | Civilian | 00/04/07 | 00/04/07 | V | Al Qaeda |
| Sombolay | Albert T. | Army | 90/12/00 | 91/03/29 | V | **Jordan, Iraq** |
| Soueid | Mohamad | Civilian | 11/03/00 | 11/10/11 | R | **Syria** |
| Souther | Glenn Michael | Civilian | 80/00/00 | 86/00/00 | V | **Soviet Union** |
| Squillacote | Theresa M. | Civilian | 80/00/00 | 97/10/07 | R | **East Germany** |
| Stand | Kurt Allen | Civilian | 72/00/00 | 97/10/04 | R | **East Germany** |
| Szabo | Zoltan | Army | 67/00/00 | 89/05/21 | R | **Hungary** |
| Thompson | Robert Glenn | Air Force | 57/06/00 | 65/00/00 | V | **Soviet Union** |
| Tobias | Bruce Edward | Civilian | 85/08/12 | 85/08/23 | V | Soviet Union |
| Tobias | Michael Timothy | Navy | 85/08/11 | 85/08/13 | V | Soviet Union |
| Trofimoff | George | Civilian | 69/00/00 | 00/06/14 | R | **Soviet Union** |
| Tsou | Douglas S. | Civilian | 86/03/00 | 88/02/09 | V | **Taiwan** |
| Tumanova | Svetlana | Civilian | 78/00/00 | 87/09/28 | R | **Soviet Union** |
| Underwood | Bryan | Civilian | 11/03/01 | 11/09/01 | V | China |
| Velazquez | Marta Rita | Civilian | 83/00/00 | 02/06/00 | R | **Cuba** |
| Verber | Otto | Civilian | 49/06/15 | 53/01/14 | R | **Soviet Union** |
| Walker | Arthur James | Civilian | 81/00/00 | 85/05/29 | R | **Soviet Union** |
| Walker, Jr. | John Anthony | Navy | 68/01/00 | 85/05/20 | V | **Soviet Union** |
| Walker | Michael Lance | Navy | 83/09/00 | 85/05/22 | R | **Soviet Union** |
| Waring | James Earnest | Air Force | 60/00/00 | 63/00/00 | R | **Soviet Union** |
| Warren | Kelly Therese | Army | 86/00/00 | 97/07/10 | R | **East Germany** |
| Weinmann | Ariel Jonathan | Navy | 05/07/00 | 06/03/26 | V | **Russia** |
| Whalen | William Henry | Army | 59/12/00 | 66/07/12 | R | **Soviet Union** |
| Whitworth | Jerry Alfred | Navy | 75/02/00 | 85/06/03 | R | **Soviet Union** |
| Williams | Herman Carleton | Air Force | 64/00/00 | 72/00/00 | V | **Soviet Union** |
| Wilmoth | James Rodney | Navy | 89/02/00 | 89/07/25 | V | Soviet Union |
| Wine | Edward Hilledon | Navy | 68/08/21 | 68/09/29 | V | Soviet Union |

APPENDIX B: LIST OF THE 209 INDIVIDUALS IN THIS STUDY AND SELECTED CHARACTERISTICS

| Surname | Given Name | Affiliation | Date Began[79] | Date of Arrest | Volunteer or Recruit | Actual or Attempted Recipient[80] |
|---|---|---|---|---|---|---|
| Wold | Hans Palmer | Navy | 83/05/00 | 83/07/21 | V | Soviet Union |
| Wolf | Ronald Craig | Civilian | 89/03/00 | 89/05/05 | V | Soviet Union |
| Wolff | Jay Clyde | Civilian | 84/12/15 | 84/12/15 | V | unknown |
| Wood | James David | Air Force | 73/03/07 | 73/07/21 | V | **Soviet Union** |
| Yai | John Joungwoong | Civilian | 97/12/00 | 03/02/04 | R | **North Korea** |